Journal of Number Theory 130 (2010) 1292–1347

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the solutions of a functional equation arising from multiplication of quantum integers

Lan Nguyen

Mathematics Department, The University of Michigan–Ann Arbor, United States

ARTICLE INFO

Article history:
Received 9 April 2007
Revised 25 February 2008
Available online 7 April 2010
Communicated by David Goss

MSC:
11P99
11C08

Keywords:
Quantum integers
Quantum polynomials
Cyclotomic polynomials
q-Series
Polynomial functional equation

ABSTRACT

This paper is the first of several papers in which we prove, for the case where the fields of coefficients are of characteristic zero, four open problems posed in the work of Melvyn Nathanson (2003) [1] concerning the solutions of a functional equation arising from multiplication of quantum integers $[n]_q = q^{n-1} + q^{n-2} + \cdots + q + 1$. In this paper, we prove one of the problems. The next papers, namely [2–4] by Lan Nguyen, contain the solutions to the other 3 problems.

1. Introduction and background

In [1], Nathanson studies the sumsets

$$\{0, 1, \ldots, m-1\} + \{0, m, \ldots, (n-1)m\} = \{0, 1, \ldots, mn-1\}$$

by considering their q-series expansions and the multiplications of expressions of the form

$$[n]_q := q^{n-1} + q^{n-2} + \cdots + q + 1,$$

E-mail address: ltng@umich.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.01.006

which he refers to as *quantum integers*; where n is in $\mathbb{N} = \{1, 2, \ldots\}$. Using the usual multiplication of polynomials for quantum integers, denoted by $[n]_q \cdot [m]_q$, we can see that it is not the same as $[nm]_q$ for general $m, n \in \mathbb{N}$. For a reasonable multiplication operation for these integers, we need to define an appropriate notion of multiplication for the corresponding polynomials. Nathanson defines one such operation, which we call *quantum multiplication* from now on and denote by $\star$:

$$[m]_q \star [n]_q = [mn]_q$$

where

$$[m]_q \star [n]_q := [m]_q \cdot [n]_{q^m}$$

for all m, n in $\mathbb{N}$. Note that $\star$ is well defined if and only if $[m]_q \star [n]_q = [mn]_q = [nm]_q = [n]_q \star [m]_q$. This is the case since it can be verified directly that $[n]_q \cdot [m]_{q^n} = [m]_q \cdot [n]_{q^m}$.

More generally, Nathanson considers sequences of polynomials $\Gamma = \{f_n(q) \mid n = 1, \ldots, \infty\}$, with coefficients contained in some field, satisfying the following functional equations:

$$f_n(q) \star f_m(q) \overset{(1)}{=} f_m(q) \star f_n(q) \overset{(2)}{=} f_{mn}(q)$$

for all $m, n \in \mathbb{N}$ and where $\star$ is the operation induced by the quantum multiplication defined above: $f_n(q) \star f_m(q) = f_n(q) f_m(q^n)$. Hereafter, we refer to the first equality in the above functional equation as Functional Equation (1) and the second equality as Functional Equation (2) or sometimes for short just (1) and (2) respectively.

Remark 1.1. It can be verified that a sequence of polynomials that satisfy Functional Equation (2) automatically satisfies Functional Equation (1) but not vice versa. For example: Let $\alpha \neq 0, 1$ and

$$\Gamma = \{f_n(q) = \alpha \mid n = 1, \ldots, \infty\}.$$

Then Γ satisfies (2) but not (1). Also, from (1) we can see that this operation is commutative.

Nathanson discusses in [1] the following problem, which is essentially the main theme of his paper:

Problem. Determine all sequences of polynomials $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ satisfying Functional Equation (2).

Let $\Gamma = \{f_n(q)\}$ be a sequence of polynomials satisfying (2). One would be interested in knowing the set of $n \in \mathbb{N}$ where $f_n(q) \neq 0$. This set of n is called the *support* of Γ and denoted by $\operatorname{supp}\{\Gamma\}$. Recall that a multiplicative semigroup of $\mathbb{N}$ is a subset A of $\mathbb{N}$ such that $1 \in A$ and $a, b \in A \Rightarrow ab \in A$. If P is a set of rational primes and A_P consists of 1 and all natural numbers such that all their prime factors come from P, then A_P is a multiplicative semigroup which is called a prime multiplicative semigroup associated to P. From [1], we know that the support of Γ is a multiplicative prime subsemigroup of $\mathbb{N}$. In fact, Nathanson proves the following theorem:

Theorem 1.2. *(See [1].) Let $\Gamma = \{f_n(q)\}$ be a sequence of polynomials satisfying Functional Equation* (2)*. Then its support,* $\operatorname{supp}\{\Gamma\}$*, is of the form A_P for some set of primes P, and Γ is completely determined by the collection of polynomials*:

$$\{f_p(q) \mid p \in P\}.$$

With this theorem, characterizing any sequence Γ satisfying Functional Equation (2) reduces to characterizing the sub-collection of polynomials with prime indexes $p \in P$. We call such a collection of primes P the **support base** of Γ. Another related result of Nathanson is used throughout our work. It provides the essential reduction in determining a solution to Functional Equation (2), with support A_P associated to a set of primes P, to that of finding a collection of polynomials indexed by P, which is a solution to Functional Equation (1).

Theorem 1.3. *(See [1].) Let P be a set of primes. Let $\Gamma' = \{f'_p(q) \mid p \in P\}$ such that*:

$$f'_{p_1}(q) \cdot f'_{p_2}\big(q^{p_1}\big) = f'_{p_2}(q) \cdot f'_{p_1}\big(q^{p_2}\big)$$

for all $p_i \in P$ (i.e., satisfying Functional Equation (1)). Then there exists a unique sequence $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ satisfying (2) such that $f_p(q) = f'_p(q)$ for all primes $p \in P$.

In the reverse direction, if P is a set of primes in $\mathbb{N}$ then there is at least one sequence Γ with $\operatorname{supp}\{\Gamma\} = A_P$. One such sequence can be defined as the set of polynomials:

$$f_m(q) = \begin{cases} [m]_q & \text{if } m \in A_P; \\ 0 & \text{otherwise.} \end{cases}$$

We say that a sequence Γ is nonzero if $\operatorname{supp}\{\Gamma\} \neq \emptyset$. If Γ satisfies Functional Equation (2), then for any $n \in \mathbb{N}$:

$$f_n(q) = f_n(q) \star f_1(q) = f_n(q) \cdot f_1(q).$$

Consequently, Γ is nonzero if and only if $f_1(q) = 1$.

The degree of each polynomial $f_n(q) \in \Gamma$ is denoted by $\deg(f_n(q))$. We know from [1] that for any nonzero sequence of polynomials Γ satisfying (2), there exists a rational number, denoted by t_Γ, such that:

$$\deg\big(f_n(q)\big) = t_\Gamma(n-1)$$

for all n in $\operatorname{supp}\{\Gamma\}$. This number t_Γ is not necessarily an integer. An example of a sequence Γ with nonintegral t_Γ can be constructed as follows: Let $P = \{p\}$ for some odd prime p, then $A_P = \{p^l \mid l \in \mathbb{N} \cup \{0\}\}$; and let $0 < r < p-1$ be in $\mathbb{N}$ such that r does not divide $(p-1)$. Then by defining $f_p(q) := q^r$, we obtain, by using Functional Equation (2) as a recursive formula, a sequence of polynomials

$$\Gamma = \big\{f_{p^l}(q) = q^{r(1+p+\cdots+p^{l-1})} = q^{\frac{r}{p-1}(p^l-1)} \,\big|\, l \in \mathbb{N} - 0\big\} \cup \big\{f_1(q) = 1\big\}$$

where $t_\Gamma = r/(p-1) \in \mathbb{Q} - \mathbb{Z}$ by construction. Later we show that t_Γ can only take on nonintegral values when the associated set of primes P consists of exactly one prime.

Another natural question to ask is how the solutions of Functional Equation (2) behave with respect to composition of polynomials as well as multiplication of polynomials. The following results are known in that respect.

Theorem 1.4. *(See [1].) Let $\Gamma = \{f_n(q)\}$ be a sequence of polynomials satisfying Functional Equation (2) and $g(q)$ be a polynomial such that $g(q^r) = g^r(q)$. Then the new sequence $\{f_n(g(q)) \mid n \in \mathbb{N}\}$ also satisfies Functional Equation (2).*

In particular, the sequence $\{f_n(q^r) \mid n \in \mathbb{N}\}$ satisfies Functional Equation (2) provided that $\{f_n(q) \mid n \in \mathbb{N}\}$ does. One important such example is the sequence of polynomials of the form:

$$f_m(q^r) := [m]_{q^r} = (q^r)^{m-1} + \cdots + (q^r) + 1,$$

for each $m \in \mathbb{N}$, which satisfies Functional Equation (2) since the sequence $\Gamma = \{[m]_q \mid m \in \mathbb{N}\}$ does.

Theorem 1.5. *If Γ_1, Γ_2 are two nonzero sequences of polynomials satisfying Functional Equation* (2)*, then the sequence $\Gamma_1 \cdot \Gamma_2$ also satisfies* (2)*. Conversely, if $\operatorname{supp}\{\Gamma_1\} = \operatorname{supp}\{\Gamma_2\}$ and Γ_1 as well as $\Gamma_1 \cdot \Gamma_2$ satisfying* (2)*, then Γ_2 also satisfies* (2)*. The collection of all solutions of Functional Equation* (2) *is an abelian semigroup. Also for every set of primes P, the set of all sequences Γ satisfying* (2) *and having support A_P forms an abelian cancellation semigroup, which is denoted by Υ_P.*

Remark 1.6. If $\Gamma_1 = \{f_n(q) \mid n \in \mathbb{N}\}$, $\Gamma_2 = \{g_n(q) \mid n \in \mathbb{N}\}$ are two nonzero sequences of polynomials satisfying Functional Equation (2), then $\Gamma_1 \cdot \Gamma_2$ is defined as the collection $\{f_n g_n(q) \mid n \in \mathbb{N}\}$ where $f_n g_n(q) = f_n(q) g_n(q)$.

One of our main goals (and also Nathanson's) is essentially to classify all the sequences of polynomials satisfying Functional Equation (2). Nathanson reduces this task, using the next result, to classify sequences of polynomials with the constant terms equal to 1.

Theorem 1.7. *(See [1].) Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a nonzero sequence of polynomials satisfying Functional Equation* (2) *with support A_P for some set of primes P. Then there exist a unique completely multiplicative arithmetic function $\psi(n)$, a rational number t, and a unique sequence $\Sigma = \{g_n(q)\}$ satisfying* (2) *with the same support A_P such that*:

$$f_n(q) = \psi(n) q^{t(n-1)} g_n(q)$$

and $g_n(0) = 1$ for all $n \in A_P$.

In studying the solutions of Functional Equation (2), Nathanson conjectures as to the essential roles of quantum integers, both as solutions of Functional Equation (2) and also as generators for these solutions in a number of important cases. In addition, he also proves this conjecture in one important case: The degree of $f_n(q)$ is equal to $n-1$ for each n, i.e., $t_\Gamma = 1$. The aim of this paper, which is described in detail in the next section, is to study the solutions of Functional Equations (1) and (2) and to resolve one of Nathanson's conjectures [1] for the case where the fields containing the coefficients of all the polynomials $f_n(q)$ are of characteristic zero.

2. Main objectives and results

2.1. Main objectives and preliminary remarks

The following open problems concerning sequences of polynomials Γ satisfying Functional Equation (2) are stated in Nathanson's paper [1] and are our main objectives. Our solutions to them, in the case where the fields of coefficients of Γ's are of characteristic zero, are given in this paper as well as our next several papers, which are currently in preparation.

As shown in [1], the sequence Γ consisting of quantum integers satisfies Functional Equation (2). It is the unique solution to this functional equation in the case where $\deg(f_n(q))$ is equal to $n-1$ for all $n \geqslant 1$ and the support of Γ contains 2 and at least one odd prime p.

The role of these integers, with respect to the solutions of Functional Equation (2), seems to extend beyond this case. In fact, Nathanson conjectures that quantum integers play an essential role in generating the general solutions of Functional Equation (2). More precisely:

Problem 1. If $t_\Gamma \geqslant 2$ and if $\deg(f_n(q)) = t_\Gamma(n-1)$ for all n in $\mathbb{N}$, then there exist integers t_i and u_i such that $t_\Gamma = \sum_i t_i u_i$ and

$$f_n(q) = \prod_i \left([n]_{q^{t_i}}\right)^{u_i}$$

for all n in the support of Γ.

Note that the condition $\deg(f_n(q)) = t_\Gamma(n-1)$ for all n in $\mathbb{N}$ means that $f_n(q)$ is nontrivial for all n in $\mathbb{N}$. As a result, a solution to this problem and the analogous result mentioned above for the case where $t_\Gamma = 1$ make it possible to express each polynomial in a large class of sequences Γ, satisfying Functional Equation (2) and with integral t_Γ, in terms of quantum integers. Thus it shows that quantum integers are in fact the building blocks for these sequences. Therefore, a solution to Problem 1 provides a very concrete tool to characterize all such sequences and also gives insights into the rest of the open problems posed in [1], which we recall below:

Problem 2. Let P be a set of rational primes. Determine all polynomial sequences $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ satisfying (2) and with support A_P.

Problem 3. Let $P \subseteq P'$ be two sets of prime numbers, and let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a sequence of polynomials satisfying (2) with support A_P. Under what condition(s) does there exist a sequence $\Gamma' = \{f'_n(q) \mid n \in \mathbb{N}\}$ with support $A_{P'}$ such that $f_p(q) = f'_p(q)$ for all $p \in P$?

Problem 4. Let Υ_P be the collection of all solutions $\{\Gamma\}$ to Functional Equation (2) having support A_P. Does every sequence of rational functions having support A_P which satisfies Functional Equation (2) belong to the Grothendieck group $K(\Upsilon_P)$ of Υ_P?

Recall that if Υ is an abelian cancellation semigroup, then there exists an abelian group $K(\Upsilon)$ and an injective semigroup homomorphism $i : \Upsilon \hookrightarrow K(\Upsilon)$ such that for any abelian group G and $\alpha : \Upsilon \hookrightarrow G$, there exists a unique group homomorphism $\alpha' : K(\Upsilon) \hookrightarrow G$ such that $\alpha = \alpha' i$. The group $K(\Upsilon)$ is called the Grothendieck group of Υ.

Before stating our main results, we discuss some important details needed for the set up of our theorems and their proofs. Then we discuss the general structure and the partition of problems among our papers.

For a sequence Γ of polynomials satisfying Functional Equation (2), the smallest field K which contains all the coefficients of all the polynomials in Γ is called **The Field of Coefficients of** Γ. We are only concerned with sequences of polynomials whose fields of coefficients K are of characteristic zero. The case of positive characteristic fields of coefficients is reserved for our future papers. Unless stated otherwise, we always view Γ as a sequence of polynomials with coefficients in a fixed separable closure $\overline{K}$ of K which is embedded in $\mathbb{C}$ via a fixed embedding $\iota : \overline{K} \hookrightarrow \mathbb{C}$. Thus every element $f(q)$ of Γ can be viewed as a polynomial in $\mathbb{C}[q]$. We frequently view polynomials $f(q)$'s in Γ as elements of the ring $\mathbb{C}[q]$ throughout this paper. Thus whenever that is necessary, it is implicitly assumed.

Since the problems above are obvious in the case where Γ is a trivial or a constant sequence, any sequence of polynomials Γ satisfying Functional Equation (2) considered in this paper is assumed to be nontrivial and nonconstant unless stated otherwise.

In this paper, we prove Problem 1 and related results since an affirmative answer to Problem 1 has important implications for the other problems. It provides the insights and tools, which are not available otherwise, to treat the rest of the problems mentioned earlier. Specifically, it becomes possible to express a general solution of Functional Equation (2), which is not concrete enough for most purposes such as classification, as a product of quantum integers which are much easier to understand. To demonstrate its utility, we show here one of its applications to the classification problem which also serves as an introduction to our next papers; the classification of all sequences of polynomials satisfying Functional Equation (2) whose supports are of the form A_P where P contains exactly one

prime number. The set of such sequences strictly contains the set of all sequences of polynomials satisfying Functional Equation (2) with t_Γ nonintegral. This result is given as a conditional result, where the condition is a theorem stated here but whose proof is postponed to our next paper.

In our next papers, namely [2–4], we prove Problems 2, 3 and 4. In Problem 2, we classify all sequences of polynomials Γ satisfying Functional Equation (2) with fields of coefficients of characteristic zero and $t_\Gamma \geqslant 1$ integral. This result, together with the classification of the sequences of polynomials discussed in the paragraph above, provides a complete classification of all sequences of polynomials satisfying Functional Equation (2) whose fields of coefficients are of characteristic zero. Note that in Problem 3 and Problem 4, the questions also cover both the case where t_Γ is integral and the case where t_Γ is fractional.

For each problem treated in these papers, we generally partition the proofs into two parts: Part 1 and Part 2, according to their fields of coefficients. Specifically Part 1 covers the case where the field of coefficients of Γ is equal to $\mathbb{Q}$, and Part 2 covers the case where $\mathbb{Q}$ is strictly contained in the field of coefficients K. In addition, we also differentiate between the cases when t_Γ is integral and when it is nonintegral and treat them accordingly.

2.2. Main results

Our main results in these papers are essentially solutions to the problems posed in [1], which are recalled earlier as Problems 1, 2, 3 and 4, for the case where the fields of coefficients of the sequences of polynomials Γ are of characteristic zero. For some of these problems, our results are stronger and more extended than what is being asked. In addition, we also prove some results related to these problems.

In this paper, we treat Problem 1. Even though Problem 1 is only concerned with the cases where $t_\Gamma \geqslant 2$, we also consider the case where $t_\Gamma = 1$.

Below are the main results in this paper:

Theorem 2.1. *Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a sequence of polynomials satisfying Functional Equation* (2) *and whose field of coefficients is of characteristic zero. Suppose $f_n(q)$ is a monic polynomial such that $f_n(0) \neq 0$ for each n in $\mathbb{N}$.*

(1) *Field of coefficients is $\mathbb{Q}$: Suppose that $\deg(f_p(q)) = t_\Gamma(p-1)$ with $t_\Gamma \geqslant 1$ for at least two distinct primes p and r, which means that the set P associated to the support A_P of Γ contains p and r and the elements $f_p(q)$ and $f_r(q)$ of Γ are nonconstant polynomials. Then there exist ordered pairs of integers $\{u_i, t_i\}_i$ with $i = 1, \ldots, s$ such that $t_\Gamma = \sum_{i=1,\ldots,s} u_i t_i$ and*

$$f_n(q) = \prod_{i=1}^{s} \left([n]_{q^{u_i}}\right)^{t_i} \tag{2.1}$$

for all n in $\mathbb{N}$.

(2) *Field of coefficients strictly contains $\mathbb{Q}$: There is no sequence of polynomials Γ, with field of coefficients strictly contains $\mathbb{Q}$, satisfying Functional Equation* (2) *and the condition $\deg(f_p(q)) = t_\Gamma(p-1)$, meaning the set P associated to the support A_P of Γ contains all prime numbers and the correspondent elements $f_p(q)$ of Γ are nonconstant polynomials, with integral $t_\Gamma \geqslant 1$ for all primes p. However, if the condition $\deg(f_p(q)) = t_\Gamma(p-1)$ with integral $t_\Gamma \geqslant 1$ for all primes p is not imposed on Γ, then there exist sequences Γ's of polynomials with fields of coefficients strictly greater than $\mathbb{Q}$ satisfying Functional Equation* (2).

The decomposition of $f_n(q)$ into a product of quantum integers as above is unique in the sense that if $\{a_j, b_j\}$ is another set of integers such that $t_\Gamma = \sum_{j=1,\ldots,h} a_j b_j$ and

$$f_n(q) = \prod_{j=1}^{h} \left([n]_{q^{a_j}}\right)^{b_j}$$

for all $n \in \operatorname{supp}\{\Gamma\}$, then for each u_i there exists at least one a_j such that $u_i = a_j$. Moreover, if $I \subseteq \{1, \ldots, s\}$ and $J \subseteq \{1, \ldots, h\}$ are two collections of indexes such that $u_i = a_j$ exactly for all i in I and j in J and nowhere else, then

$$\sum_{i \in I} t_i = \sum_{j \in J} b_j,$$

and the above relation between any such set of integers $\{a_j, b_j\}_j$ and the set $\{u_i, t_i\}_i$ is an equivalence relation.

Remark 2.2. The result we obtain above is stronger than what is being conjectured in Problem 1 in the case where the field of coefficients is $\mathbb{Q}$. The support of Γ is only required to contain any two distinct primes, instead of all primes as required in the hypothesis of Problem 1. Even though the case $t_\Gamma = 1$ is proved by Nathanson without the restriction on the characteristic of the fields of coefficients, our solution for this case does not require the support of Γ to contain 2 as in Theorem 8 and Theorem 9 of [1]. Moreover, our technique can be generalized to all fields of coefficients of characteristic zero as well as the case where t_Γ is nonintegral. In addition, this theorem also provides the range of possible variations of the sets of integers $\{u_i, t_i\}$'s and thus gives a characterization of such decompositions. We denote an equivalent class of $\{u_i, t_i\}_i$, with respect to the above equivalence relation, by $\|\{u_i, t_i\}_i\|$.

Before we give an application of Theorem 2.1, we state another theorem which provides a close relationship between sequences of polynomials satisfying Functional Equation (2) with fields of coefficients $\mathbb{Q}$ and those with fields of coefficients strictly greater than $\mathbb{Q}$. We postpone its proof since it is one of the main results of our next papers.

Theorem 2.3. *Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a sequence of polynomials with field of coefficients of characteristic zero and satisfying Functional Equation* (2)*. Suppose that the set of primes P associated to the support of Γ contains at least two distinct primes. Then there exists a sequence $\Gamma' = \{f'_n(q) \mid n \in \mathbb{N}\}$ of polynomials satisfying Functional Equation* (2) *with field of coefficients equal to $\mathbb{Q}$ and $\operatorname{supp}\{\Gamma\} = \operatorname{supp}\{\Gamma'\}$ such that $f_n(q)$ divides $f'_n(q)$ in $\mathbb{C}[q]$ for all n in $\operatorname{supp}\{\Gamma\}$, $t_{\Gamma'} - t_\Gamma \in \mathbb{N} \cup \{0\}$.*

The next corollary is a consequence of both Theorem 2.1 and 2.3 above. It makes it possible to characterize sequences Γ with t_Γ nonintegral by providing a crucial limitation on the possibility of t_Γ being nonintegral.

Corollary 2.4. *Let Γ be a sequence of polynomials satisfying Functional Equation* (2) *with field of coefficients of characteristic zero and support A_P where P is a set of primes. Then t_Γ is integral if $|P| \geqslant 2$ where $|P|$ is the cardinality of P.*

Theorem 2.5.

(a) *If the parameter t_Γ of a sequence of polynomials $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$, satisfying Functional Equation* (2) *and with field of coefficients of characteristic zero, is nonintegral, then the set of primes P associated to the support A_P of Γ contains exactly one prime.*

(b) *If $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ is a sequence of polynomials satisfying Functional Equation* (2)*, whose field of coefficients is of characteristic zero and t_Γ nonintegral, then Γ is completely determined by the polynomial $f_p(q)$ where p is the prime in the support of Γ. In the opposite direction, for each triple $(f(q), p, t)$ where p is a prime, $f(q)$ is any monic polynomial with coefficients in the field of characteristic zero, nonzero constant term and of degree td where d is any divisor of $p-1$ such that $(t, \frac{p-1}{d}) = 1$, there exists a unique sequence of polynomials $\Gamma = \{f_{p^n}(q) \mid n \in \mathbb{N};\ f_{p^0}(q) = 1,\ f_{p^1}(q) = f(q)\}$, with the same field of coefficients as $f(q)$, which satisfies Functional Equation* (2)*.*

Remark 2.6. Theorem 2.5 gives a complete characterization of all sequences Γ of polynomials with fields of coefficients of characteristic zero, satisfying Functional Equation (2) and t_Γ nonintegral. As a

result, what remains to be done in Problem 2 is to classify all sequences of polynomials with integral t_Γ parameter.

Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a sequence of polynomials with field of coefficients of characteristic zero, satisfying Functional Equation (2). If there exist ordered pairs of integers $\{u_i, t_i\}_i$ with $i = 1, \ldots, s$ such that $t_\Gamma = \sum_{i=1,\ldots,s} u_i t_i$ and $f_n(q)$ satisfy (2.1) for each n in the support of Γ, then we say that Γ is **generated** by quantum integers. We say that Γ is **weakly generated** by quantum integers if $f_n(q)$ can be written as a product of quantum integers for each n in the support of Γ. Note that being generated by quantum integers implies being weakly generated by quantum integers but not necessarily vice versa. If Γ is weakly generated by quantum integers but not generated by quantum integers, we say that Γ is **strictly weakly generated** by quantum integers. In the same spirit as Theorem 2.1, the next result shows the extent to which quantum integers serve as generators of sequences of polynomials satisfying Functional Equation (2) in the case of nonintegral t_Γ parameter. By Corollary 2.4, such Γ must have support of the form $\{p^n \mid n \in \mathbb{N}\}$.

Theorem 2.7. *Let $\Gamma = \{f_{p^n}(q) \mid p \in \operatorname{supp}\{\Gamma\},\ n \in \mathbb{N}\}$ be a sequence of polynomials with field of coefficients of characteristic zero, satisfying Functional Equation* (2) *and with t_Γ nonintegral. Then Γ cannot be generated by quantum integers. It is strictly weakly generated by quantum integers if and only if*

$$\Gamma = \prod_i (\Gamma_i)^{n_i}$$

where n_i is positive integer and Γ_i is a sequence of polynomials satisfying Functional Equation (2)*, which is generated by quantum integers, for each i. Such decomposition of Γ as a product of sequences Γ_i's is unique in the following sense*:

(1) *If $f_n(q)$ and $f_m(q)$ are polynomials in Γ_i, then roots of $f_n(q)$ and $f_m(q)$ are primitive roots of unity of the same order.*
(2) *If $f_n(q)$ and $f_m(q)$ are polynomials in Γ_i and Γ_j respectively for $i \neq j$, then roots of $f_n(q)$ and $f_m(q)$ are primitive roots of unity of distinct orders.*

3. Proof of main results

To show that Theorem 2.1 in fact gives a solution to Problem 1, we need to show that the hypothesis $f_n(0) = 1$ for all natural numbers n can be equivalently replaced by the hypothesis $f_n(q)$ is a monic polynomial with $f_n(0) \neq 0$ each natural number n.

First we need the following reduction result which is similar to Theorem 1.7.

Proposition 3.1. *Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a nonzero sequence of polynomials satisfying Functional Equation* (2) *with support A_P for some set of primes P. Then there exist a unique completely multiplicative arithmetic function $\psi(n)$, a rational number t, and a unique sequence $\Sigma = \{g_n(q)\}$ satisfying* (2) *with the same support A_P such that*

$$f_n(q) = \psi(n) q^{t(n-1)} g_n(q)$$

where $g_n(q)$ is a monic polynomial with $g_n(0) \neq 0$ for all $n \in A_P$.

Proof. Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a nonzero sequence of polynomials satisfying Functional Equation (2) with support A_P for some set of primes P. For each $f_n(q)$ in Γ, let $\psi(n)$ be the leading coefficient of $f_n(q)$ and let q^{α_n} be the highest power of q dividing $f_n(q)$. Define

$$g_n(q) = \frac{f_n(q)}{\psi(n) q^{\alpha_n}}.$$

Then $g_n(q)$ is a monic polynomial such that $g_n(0) \neq 0$. It follows immediately from our definition of $g_n(q)$ that

$$g_n(q) \neq 0 \quad \Leftrightarrow \quad f_n(q) \neq 0.$$

Hence if $\Gamma' = \{g_n(q) \mid n \in \mathbb{N}\}$ satisfies Functional Equation (2), then Γ' has the same support as Γ, namely A_P. Next, let m and n be any two natural numbers in A_P. Then

$$f_{mn} = f_m(q) f_n\big(q^m\big) = f_m(q) f_n\big(q^m\big).$$

Hence

$$\begin{aligned}\psi(mn) q^{\alpha_{mn}} g_{mn}(q) &= \psi(m) q^{\alpha_m} g_m(q) \psi(n) \big(q^m\big)^{\alpha_n} g_n\big(q^m\big) \\ &= \psi(n) q^{\alpha_n} g_n(q) \psi(m) \big(q^n\big)^{\alpha_m} g_m\big(q^n\big),\end{aligned}$$

or equivalently

$$\begin{aligned}\psi(mn) q^{\alpha_{mn}} g_{mn}(q) &= \psi(m)\psi(n) q^{\alpha_m + m\alpha_n} g_m(q) g_n\big(q^m\big) \\ &= \psi(n)\psi(m) q^{\alpha_n + n\alpha_m} g_n(q) g_m\big(q^n\big).\end{aligned}$$

Since $g_m(q)$, $g_n(q)$ and $g_{mn}(q)$ are monic polynomials with nonzero constant terms, $g_m(q) g_n(q^m)$ and $g_n(q) g_m(q^n)$ are also monic polynomials with nonzero constant terms. As a result, it can be verified that the following must hold:

(1) $\psi(mn) = \psi(m)\psi(n)$.
(2) $q^{\alpha_{mn}} = q^{\alpha_m + m\alpha_n} = q^{\alpha_n + n\alpha_m}$.
(3) $g_{mn}(q) = g_m(q) g_n(q^m) = g_n(q) g_m(q^n)$.

It follows from (2) that

$$\alpha_{mn} = \alpha_m + m\alpha_n = \alpha_n + n\alpha_m.$$

Hence

$$\alpha_m(n-1) = \alpha_n(m-1),$$

or equivalently,

$$\frac{\alpha_m}{m-1} = \frac{\alpha_n}{n-1} = t.$$

Therefore

$$\alpha_n = t(n-1)$$

for each natural number n and the result follows. □

Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a sequence of polynomials satisfying Functional Equation (2) such that its field of coefficients is of characteristic zero and $f_n(0) = 1$. By Proposition 3.1, there exist a unique

completely multiplicative arithmetic function $\psi(n)$, a rational number t, and a unique sequence $\Sigma = \{g_n(q)\}$ satisfying (2) with the same support as that of Γ such that

$$f_n(q) = \psi(n)q^{t(n-1)}g_n(q)$$

where $g_n(q)$ is a monic polynomial with $g_n(0) \neq 0$ for each $n \in \operatorname{supp}\{\Gamma\}$. As a result, there exist ordered pairs of integers $\{u_i, t_i\}_i$ with $i = 1, \ldots, s$ such that $t_\Gamma = \sum_{i=1,\ldots,s} u_i t_i$ and

$$f_n(q) = \prod_{i=1}^{s} \left([n]_{q^{u_i}}\right)^{t_i}$$

for all n in $\mathbb{N}$ if and only if

$$g_n(q) = \prod_{i=1}^{s} \left([n]_{q^{u_i}}\right)^{t_i}$$

for all n in the support of Γ. Therefore, the condition $f_n(0) = 1$ *for all* n *in* $\mathbb{N}$ in Problem 1 is equivalent to the condition $f_n(q)$ *is monic with nonzero constant term for all* n *in* $\mathbb{N}$ in Theorem 2.1. From now on, we only consider, unless otherwise stated, sequences of polynomials, which are monic and have nonzero constant terms, satisfying Functional Equation (2) with field coefficients of characteristic zero.

Proposition 3.2. *Let Γ be a sequence of polynomials with field of coefficients of characteristic zero, satisfying Functional Equation* (2) *and whose support consists of at least two distinct primes. Let p be any prime in* $\operatorname{supp}\{\Gamma\}$, *and let $f_p(q)$ be the corresponding polynomial in Γ. Let α be any root of $f_p(q)$. Then α is a root of unity of order divisible by p.*

Proof. Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a sequence of polynomials, with coefficients in a field of characteristic zero, which is a solution to Functional Equation (2). Let p and r be two distinct prime numbers in $\operatorname{supp}\{\Gamma\}$ which contain at least two distinct primes by hypothesis. Then by Functional Equation (2) we have

$$f_{pr}(q) = f_p(q)f_r\left(q^p\right) \overset{(\star)}{=} f_r(q)f_p\left(q^r\right).$$

First let us view every element of Γ as an element of the ring $\mathbb{C}[q]$. Let α be a root of $f_p(q)$. Then $\alpha^{\frac{1}{r}}$ is a root of $f_p(q^r)$ for any r-root $\alpha^{\frac{1}{r}}$ of α. From $(\star)$, we have two cases:

(1) Either $\alpha^{\frac{1}{r}}$ is a root of $f_p(q)$ or
(2) $\alpha^{\frac{1}{r}}$ is a root of $f_r(q^p)$.

If the first case occurs, we can repeat this process with α replaced by $\alpha^{\frac{1}{r}}$. Otherwise, (2) implies that $\alpha^{\frac{p}{r}}$ is a root of $f_r(q)$. Again from $(\star)$, we also have two cases:

(a) Either $\alpha^{\frac{p}{r}}$ is a root of $f_p(q)$ or
(b) $\alpha^{\frac{p}{r}}$ is a root of $f_r(q^p)$.

As before, if case (a) occurs, we repeat the process with α replaced by $\alpha^{\frac{p}{r}}$ as a root of $f_p(q)$. If case (b) occurs, then $\alpha^{\frac{p^2}{r}}$ would be a root of $f_r(q)$ and we can use the process again as in case (2) above with $\alpha^{\frac{p^2}{r}}$ replacing $\alpha^{\frac{p}{r}}$.

Therefore, there is an infinite number of rational numbers of the form $\frac{p^h}{r^g}$ with h, g integers such that $\alpha^{\frac{p^h}{r^g}}$ is either a root of $f_p(q)$ or $f_r(q)$. Since these polynomials have only a finite number of roots, the outcomes of the process must eventually repeat. Thus there must exist integers h, g, h', g' such that

$$\alpha^{\frac{p^h}{r^g}} = \alpha^{\frac{p^{h'}}{r^{g'}}}$$

or equivalently,

$$\alpha^{\frac{p^h}{r^g} - \frac{p^{h'}}{r^{g'}}} = 1.$$

Hence α is a root of unity as desired.

To prove that p divides the order, as a root of unity, of any root α of $f_p(q)$, we make a comparison of the roots of the polynomials on both sides of the equality $(\star)$ above. Let us view the field of coefficients of Γ as a subfield of $\mathbb{C}$ via ι. Then the polynomials on both sides of $(\star)$ can be split into linear factors. Since all roots of $f_p(q)$ and $f_r(q)$ are roots of unity, we can write

$$f_p(q) = \prod_{m_x > m_{x+1}} f_{m_x}(q)$$

and

$$f_r(q) = \prod_{n_y > n_{y+1}} f_{n_y}(q)$$

where roots of $f_{m_x}(q)$ (resp. $f_{n_y}(q)$) are all the roots of $f_p(q)$ and $f_r(q)$ which are roots of unity of order m_x (resp. n_y). If α is a root of $f_r(q)$, then α is a root of $f_{n_l}(q)$ for some n_l. Since α can be viewed as in $\mathbb{C}$, it can be written as $\alpha = e^{\frac{2\pi i s}{n_l}}$ where $0 \leqslant s < n_l$ and $(s, n_l) = 1$. Thus the set $\mathcal{A}$ of all p-roots of α can be written as

$$\mathcal{A} = \left\{ e^{\frac{2\pi i(s+kn_l)}{n_l p}} \;\middle|\; 0 \leqslant k < p \right\}.$$

It can be verified that if p divides n_l, then each element of $\mathcal{A}$ is a root of unity of order $n_l p$. Otherwise there is exactly one element of $\mathcal{A}$ which is root of unity of order n_l but the other $p-1$ elements of $\mathcal{A}$ are roots of unity of order $n_l p$. Note that every element of $\mathcal{A}$ is a root of $f_{n_l}(q^p)$. Therefore, if $f_{n_l}(q^p)$ possesses at least one root which is a root of unity of order n_l, then it possesses exactly as many roots which are roots of unity of order n_l as the degree of $f_{n_l}(q)$.

Definition 3.3. Let $f_{m_x}(q)$ (resp. $f_{n_y}(q)$) be a factor of $f_p(q)$ (resp. $f_r(q)$). Let S_{m_x} (resp. $S^p_{n_y}$) be the set of roots of $f_{m_x}(q)$ (resp. $f_{n_y}(q)$). The set of all r-roots (resp. p-roots) of every element of S_{m_x} (resp. S_{n_y}) is partitioned into two subsets denoted by $\mathcal{H}^{(r)}_{m_x}$ and $\mathcal{L}^{(r)}_{m_x}$ (resp. $\mathcal{H}^{(p)}_{n_y}$ and $\mathcal{L}^{(p)}_{n_y}$) where each element of $\mathcal{H}^{(r)}_{m_x}$ (resp. $\mathcal{H}^{(p)}_{n_y}$) is a root of unity of order $m_x r$ (resp. $n_y p$) and each element of $\mathcal{L}^{(r)}_{m_x}$ (resp. $\mathcal{L}^{(p)}_{n_y}$) is a root of unity of order m_x (resp. n_y). Elements of $\mathcal{H}^{(r)}_{m_x}$ and $\mathcal{L}^{(r)}_{m_x}$ are called the **high** r-roots and **low** r-roots of S_{m_x} (resp. elements of $\mathcal{H}^{(p)}_{n_y}$ and $\mathcal{L}^{(p)}_{n_y}$ are called **high** and **low** p-roots of S_{n_y}).

Remark 3.4. For each m_x and n_y, $\mathcal{H}^{(r)}_{m_x}$ and $\mathcal{H}^{(p)}_{n_y}$ are nonempty, but it is not necessarily true that either $\mathcal{L}^{(r)}_{m_x}$ or $\mathcal{L}^{(p)}_{n_y}$ is nonempty. We also refer to an element of $\mathcal{H}^{(r)}_{m_x}$ (resp. $\mathcal{H}^{(p)}_{n_y}$) as a high root of $f_{m_x}(q^r)$ (resp. a high root of $f_{n_y}(q^p)$).

Now let us write Functional Equation (1) in an expanded form as follows:

$$\begin{array}{cc} f_{m_1}(q) f_{n_1}\big(q^p\big) & f_{n_1}(q) f_{m_1}\big(q^r\big) \\ \cdots & \cdots \\ f_{m_k}(q) f_{n_l}\big(q^p\big) & f_{n_l}(q) f_{m_k}\big(q^r\big) \\ \cdots & \cdots \\ f_p(q) f_r\big(q^p\big) & \overset{(1)}{=} \quad f_r(q) f_p\big(q^r\big) \end{array}$$

where $f_p(q) f_r(q^p)$ and $f_r(q) f_p(q^r)$ are equal to the product of polynomials in the column above it.

If $m = \max\{m_1, n_1 p\}$, then m is greater than m_x and $n_y p$ for all x and y since $m_x > m_{x+1}$ and $n_y > n_{y+1}$ for all x, y by assumption. Similarly, if $m' = \max\{n_1, m_1 r\}$, then m' is greater than n_y and $m_x p$ for all x and y. Therefore, there exists a root π of $f_p(q) f_r(q^p)$ which is a root of unity of order m. On the other hand, there also exists a root π' of $f_r(q) f_p(q^r)$ of order m'. Since π and π' are roots of $f_p(q) f_r(q^p)$ and $f_r(q) f_p(q^r)$ respectively of maximum order as roots of unity, we have $m = m' = n_1 p = m_1 r$. Therefore, p divides m_1. Now suppose that p divides m_x for all $x < k$ for some positive integer k. We may assume that $f_{m_k}(x)$ divides $f_p(q)$ since there is nothing to prove otherwise. Let α be a high root of $f_{m_k}(q^r)$. Then its order is $m_k r$. There are three cases:

(1) α is a root of $m_l(q)$ for some $l < k$. If this is the case then p divides $m_k r = m_l$ by assumption. Thus p divides m_k.
(2) If α is a high root of $f_{n_l}(q^p)$ for some n_l, then p divides $n_l p = m_k$.
(3) If α is a low root of $f_{n_l}(q^p)$ for some n_l, then it is a root of unity of order n_l and thus $n_l = m_k r$. Suppose that (1) and (2) do not occur. From our analysis immediately above Definition 3.2, there must then exist a root β of $f_{n_l}(q)$ which is either a root of $f_{m_r}(q)$ for some $r < k$ or a hight root of $f_{n_s}(q^p)$ for some $n_s < n_l$. Then p divides $m_r = n_s p = m_k r$ by assumption. Therefore, p divides m_k.

As a result, if α is a root of $f_p(q)$, then it is a root of unity of order divisible by p. Thus the proof of the proposition is complete. □

Proposition 3.5. *Let Γ be a sequence of polynomials satisfying Functional Equation* (2) *with $\mathbb{Q}$ as its field of coefficients. Let $f_n(q)$ be any nonzero polynomial in Γ. Then there exists a collection of finitely many integers $\{a_j, b_j\}_j$ such that*:

$$f_n(q) = \prod_j \big([n]_{q^{a_j}}\big)^{b_j}.$$

Proof. Let $f_p(q)$ be a polynomial in Γ for some prime p in $\operatorname{supp}\{\Gamma\}$. From the discussion in previous sections, it is sufficient that we prove this proposition for an arbitrary prime in the support of Γ; and for this it is again sufficient if we prove the proposition for any irreducible factor of $f_p(q)$ and then take their product. Let α be any root of $f_p(q)$. Then by Proposition 4.3, α is a nontrivial root of unity. Let g be the order of α, i.e. g is the smallest positive integer such that $\alpha^g = 1$. Thus by Proposition 3.3, p divides g. Let $m_{\alpha,\mathbb{Q}}(q)$ be the minimal polynomial of α over $\mathbb{Q}$. Then $m_{\alpha,\mathbb{Q}}(q)$ is a monic irreducible polynomial over $\mathbb{Q}$ such that $m_{\alpha,\mathbb{Q}}(\alpha) = 0$ and $m_{\alpha,\mathbb{Q}}(q)$ divides $f_p(q)$. Therefore, $m_{\alpha,\mathbb{Q}}(q)$ must be the cyclotomic polynomial of order g. It suffices for us to prove that $m_{\alpha,\mathbb{Q}}(q)$ can

be written as $\prod_i ([p]_{q^{x_i}})^{y_i}$ for some collection of integers $\{x_i, y_i\}_i$. We prove this by induction on the number of prime factors, with multiplicity, of g where g is divisible by p.

Since $m_{\alpha,\mathbb{Q}}(q)$ divides $q^g - 1$ which can be factored as

$$q^g - 1 = (q-1)\big(q^{g-1} + \cdots + q + 1\big),$$

$m_{\alpha,\mathbb{Q}}(q)$ must divide $(q^{g-1} + \cdots + q + 1)$ since 1 is not a root of $f_p(q)$. Let $g = \prod_{i=1}^{s} p_i^{l_i}$ be the prime factorization of g which is indexed in such a way that $p = p_s$. Let us consider the following factorization of $q^{g-1} + \cdots + q + 1$:

$$\prod_{i=0}^{l_1-1}\big(\big(q^{p_1^i}\big)^{p_1-1} + \cdots + \big(q^{p_1^i}\big) + 1\big) \prod_{i=0}^{l_2-1}\big(\big(q^{p_1^{l_1} p_2^i}\big)^{p_2-1} + \cdots + \big(q^{p_1^{l_1} p_2^i}\big) + 1\big)$$
$$\cdots \prod_{i=0}^{l_s-1}\big(\big(q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^i}\big)^{p_s-1} + \cdots + \big(q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^i}\big) + 1\big).$$

Then $m_\alpha(q)$ must divide $((q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}})^{p_s-1} + \cdots + (q^{\prod_{j=1}^{s-1} p_j^{l_j}} q^{p_s^{l_s-1}}) + 1)$, the last factor which we refer to from now on as the rightmost factor in such factorizations, but no other factors to the left of it since $m_{\alpha,\mathbb{Q}}(q)$ is irreducible and g is the smallest positive integer such that α is a root of $q^g - 1 = 0$. Our goal now is to extract $m_{\alpha,\mathbb{Q}}(q)$ out of this last factor.

Remark 3.6. Every factor in the above factorization as well as every factor in all the similar factorizations of $r = \prod_i p_i^{l_i}$, obtained by permutations of the indexes i's, is of the form $[m]_{q^n}$ for some integers n and m.

Let us consider all roots of $((q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}})^{p_s-1} + \cdots + (q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}}) + 1)$. They are all the $g = \prod_{i=1}^{s} q_i^{l_i}$-roots of unity which are not $(\prod_{j=1}^{s-1} p_j^{l_j}) p_s^{l_s-1}$-roots of unity since:

$$\frac{q^g - 1}{q^{(\prod_{j=1}^{s-1} p_j^{l_j}) p_s^{l_s-1}} - 1} = \big(\big(q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}}\big)^{p_s-1} + \cdots + \big(q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}}\big) + 1\big).$$

Let us define the following collection of products:

$$\mathcal{A} = \left\{ \left(\prod_{j\in J} p_j^{d_j} \right) p_s^{l_s} \;\middle|\; J \subseteq \{1, \ldots, s-1\};\ 0 \leqslant d_j \leqslant l_j;\ \sum_{j\in J} d_j < \left(\sum_{j=1}^{s-1} l_j \right) - 1 \right\}.$$

Then $\mathcal{A}$ has the property that $p = p_s$ divides each element of $\mathcal{A}$.

For each $a \in \mathcal{A}$, let $P_a(q)$ be the cyclotomic polynomial with coefficients in $\mathbb{Q}$ of order a, i.e., the irreducible monic polynomial over $\mathbb{Q}$ whose roots are all primitive roots of unity of order a.

Lemma 3.7. *All cyclotomic polynomials over $\mathbb{Q}$ of order at least 2 are generated by expressions of the form $[m]_{q^n}$ for some integers n and m.*

Proof. We prove this by induction on the number of prime factors, with multiplicity, of a, the order of the corresponding cyclotomic polynomial $P_a(q)$:

(1) Suppose $a = p$, i.e. it is a product of only one prime factor. Then $P_a(q) = q^{p-1} + \cdots + q + 1 = [p]_q$ is the cyclotomic polynomial of order p by Eisenstein criterion.

(2) Suppose $a = \prod_{j\in J} p_j^{d_j}$ with $\sum_{j\in J} d_j = k$, i.e. a is a product of k prime factors which are not necessarily distinct. Let us consider the collection of cyclotomic polynomials $\{P_{a/d}(q)\}$ where d is a divisor of a different from 1 and d, i.e., a nontrivial divisor of a. Thus the number of prime factors of $\frac{a}{d}$ is strictly smaller than k for all such d. By induction, these cyclotomic polynomials are generated by the expressions of the form $[m]_{q^n}$ where n and m are integers. Moreover, the cyclotomic polynomials $\{P_{a/d}(q)\}$ are mutually relatively prime in $\mathbb{C}[q]$ and they all divide the polynomial $P(q) = q^{a-1} + \cdots + q + 1 = [a]_q$. Since $P_a(q)$ can be written as

$$P_a(q) = \frac{P(q)}{\prod_d P_{a/d}(q)}$$

where d runs over all nontrivial divisors of a, $P_a(q)$ is expressed as a product of expressions of the form $[m]_{q^n}$ where n and m are integers as required. □

Lemma 3.8. *Let a be in $\mathcal{A}$. Let $P_a(q)$ be the corresponding cyclotomic polynomial. Then $m_{\alpha,\mathbb{Q}}(q)$ does not divide $P_a(q)$ for any $a \in \mathcal{A}$.*

Proof. By construction, every root of $m_{\alpha,\mathbb{Q}}(q)$ is a root of unity of order g. On the other hand, every root of $P_a(q)$ is a root of unity of order a, which is strictly less than g by construction since we require that $\sum_{j\in J} d_j < (\sum_{j=1}^{s} l_j) - 1$ in the definition of $\mathcal{A}$, for each $a \in \mathcal{A}$. Thus the result follows. □

As a result of Lemma 3.7 and Lemma 3.8, $m_\alpha(q)$ must divide

$$\frac{((q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}})^{p_s-1} + \cdots + (q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}}) + 1)}{\prod_{a\in\mathcal{A}} P_a(q)}.$$

Lemma 3.9.

$$\frac{((q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}})^{p_s-1} + \cdots + (q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}}) + 1)}{\prod_{a\in\mathcal{A}} P_a(q)}$$

is the cyclotomic polynomial of order g over $\mathbb{Q}$ and thus is irreducible.

Proof. The numerator of the rational function above is a monic polynomial whose roots are all $\prod_{i=1}^{s} p_i^{l_i} = g$-roots of unity which are not $(\prod_{i=1}^{s-1} p_i^{l_i}) p_s^{l_s-1}$-roots of unity. On the other hand, roots of $\prod_{a\in\mathcal{A}} P_a(q)$ are all roots of unity of order properly dividing g but not dividing $(\prod_{i=1}^{s-1} p_i^{l_i}) p_s^{l_s-1}$ since $p_s^{l_s}$ divides a but does not divide $(\prod_{i=1}^{s-1} p_i^{l_i}) p_s^{l_s-1}$. Therefore, roots of $\frac{((q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}})^{p_s-1} + \cdots + (q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}}) + 1)}{\prod_{a\in\mathcal{A}} P_a(q)}$ are all primitive g roots of unity. It is also a monic polynomial. As a result, $\frac{((q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}})^{p_s-1} + \cdots + (q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}}) + 1)}{\prod_{a\in\mathcal{A}} P_a(q)}$ must be the cyclotomic polynomial of order g with coefficients in $\mathbb{Q}$ and hence irreducible over $\mathbb{Q}$. □

Therefore we have

$$m_\alpha(q) = \frac{((q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}})^{p_s-1} + \cdots + (q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}}) + 1)}{\prod_{a\in\mathcal{A}} P_a(q)}.$$

Now the numerator can also be written as

$$[p_s]_{q^{(\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1})}} = [p]_{q^{(\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1})}}.$$

By Lemma 3.6 and induction hypothesis, each factor $P_a(q)$ in the denominator can also be written in the form $\prod_i ([p_s]_{q^{\gamma z_{i,a}}})^{w_{i,a}} = \prod_i ([p]_{q^{\gamma z_{i,a}}})^{w_{i,a}}$ for some integers $z_{i,a}$ and $w_{i,a}$ since p_s divides a for each a in $\mathcal{A}_g$ by construction and the number of prime factors of a is strictly less than g. Therefore, $m_{\alpha,\mathbb{Q}}(q)$ can be written as

$$m_{\alpha,\mathbb{Q}}(q) = \prod_i \left([p]_{q^{x_i}}\right)^{y_i}$$

for integers x_i and y_i. Finally, by taking the product of all the irreducible factors of $f_p(q)$, we arrive at our desired conclusion. □

Let us return to the proof of Theorem 2.1, which we divide into two parts:

Part 1. The field of coefficients of Γ is $\mathbb{Q}$.

To prove Theorem 2.1 for this case, all that is left to be shown at this point are the following statements:

(1) There exists a collection $\{a_i, b_i\}_{i=1,\dots,g}$ such that $t_\Gamma = \sum_{i=1}^{g} a_i b_i$ and

$$f_n(q) = \prod_{i=1}^{g} \left([n]_{q^{a_i}}\right)^{b_i}$$

for all $n \in \operatorname{supp}\{\Gamma\}$.

(2) The uniqueness of the decomposition in the sense described in the statement of Theorem 2.1.

For the convenience of our argument, we prove (2) before we prove (1). Suppose that there exist two distinct sets of integers $\{a_i, b_i\}_i$ and $\{c_j, d_j\}_j$ such that:

- $t_\Gamma = \sum_i a_i b_i = \sum_j c_j d_j$.
- $f_n(q) = \prod_i ([n]_{q^{a_i}})^{b_i} = \prod_j ([n]_{q^{c_j}})^{d_j}$ for all n is $\operatorname{supp}\{\Gamma\}$.

If there exists one index k such that $a_k > \max_j\{c_j\}$. Then $\prod_i ([n]_{q^{a_i}})^{b_i}$ possesses at least one na_k-primitive-root of unity while $\prod_j ([n]_{q^{c_j}})^{d_j}$ does not since the order of the roots of unity, which are solutions of $\prod_j ([n]_{q^{c_j}})^{d_j}$, are at most $n(\max_j\{c_j\})$. Thus we get a contradiction. The situation is exactly the same if there exists an index l such that $c_l > \max_i\{a_i\}$. Therefore if $a_k := \max_i\{a_i\}$, then $a_k = c_l = \max_j\{c_j\}$. Let us define $M := \{[n]_{q^{a_i}} \mid a_i = a_k\}$ and $N := \{[n]_{q^{c_j}} \mid c_j = c_l\}$ with multiplicity.

Lemma 3.10. *Let $|\cdot|$ denote the cardinality function. Then $|M| = |N|$.*

Proof. Suppose $|M| < |N|$. Then we divide all the factors $([n]_{q^{a_i}})^{b_i}$ with $a_i \in M$ from both sides of

$$\prod_i \left([n]_{q^{a_i}}\right)^{b_i} \overset{(\star)}{=} \prod_j \left([n]_{q^{c_j}}\right)^{d_j}.$$

Then by our assumption, there must remain at least one factor of $[n]_{q^{c_j}}$ with $c_j \in N$ on the right-hand side (RHS). Consequently, the RHS possesses at least one primitive nc_l-roots of unity while the LHS does not. It is thus a contradiction. As a result, we have

$$\sum_{i,a_i\in M} b_i = |M| = |N| = \sum_{j,c_j\in N} d_j.$$

The whole process can be repeated after we divide both sides of $(\star)$ by the product

$$\prod_{a_i\in M} \left([n]_{q^{a_i}}\right)^{b_i}.$$

Therefore the result follows. □

From above, the statement concerning the equivalence relation in Theorem 2.1 follows immediately. Moreover, it also follows that if $f_n(q)$ is generated in the above fashion with respect to the set of integers $\{u_i, t_i\}_i$, then it is also generated in such manner with any collection of integers in the equivalent class $\|\{u_i, t_i\}_i\|$ of $\{u_i, t_i\}_i$.

To prove (1), let us suppose the contrary. By Proposition 3.5, there exist integers $m < n$ and a set $T = \{\{a_i, b_i\}_i \mid f_j(q) = \prod_i ([j]_{q^{a_i}})^{b_i}\ \forall j \leqslant m,\ t_\Gamma = \sum_i a_i b_i\} \neq \emptyset$ and that $f_n(q) \neq \prod_i ([n]_{q^{a_i}})^{b_i}$ for all $\{a_i, b_i\}_i \in T$. Also by Proposition 3.5, there exists a collection of integers $\{c_j, d_j\}_j$ with $t_\Gamma = \sum_j c_j d_j$ such that $f_n(q) = \sum_j ([n]_{q^{c_j}})^{d_j}$. By our assumption, $\{c_j, d_j\}_j$ is different from any $\{a_i, b_i\}_i \in T$.

By Functional Equation (1) we have $f_m(q) f_n(q^m) = f_n(q) f_m(q^n)$ and thus

$$\prod_i \left([m]_{q^{a_i}}\right)^{b_i} \left\{ \prod_j \left([n]_{(q^m)^{c_j}}\right)^{d_j} \right\} \overset{(*)}{=} \prod_j \left([n]_{q^{c_j}}\right)^{d_j} \left\{ \prod_i \left([m]_{(q^n)^{a_i}}\right)^{b_i} \right\}$$

for some collection of tuples $\{a_i, b_i\}_i \in T$. It can be verified that the highest order of the primitive roots of unity which are roots of the LHS and RHS come from the factors inside the brackets $\{\cdot\}$. The order of the roots of unity of highest order on the LHS is $nm(\max_j\{c_j\})$ while the order of the roots of unity of highest order on the RHS is $nm(\max_i\{a_i\})$. Using the same method as in the proof of (2) and Proposition 3.1, we can deduce that $v := \max_j\{c_j\} = \max_i\{a_i\}$ as well as

$$A := \sum_{\{j|c_j=v\}} d_j = \sum_{\{i|a_i=v\}} b_i.$$

A direct replication of the method of the proof of Lemma 3.10 above in which we divide both sides of $(*)$ by the factor $\prod_{a_j=v} ([n]_{q^{a_j}})^{b_j} = \prod_{c_i=v} ([n]_{q^{c_i}})^{d_i}$ does not work here. This is because we cannot repeat this process as in the proof of (2) due to the complications that stem from the occurrence of the other factors. Nonetheless, we can circumvent this problem in the following manner: From before, we know that roots of $[n]_{(q^m)^v}$ are all nmv-roots of unity that are not mv-roots of unity while roots of $[m]_{q^v}$ are all mv-roots of unity that are not v-roots of unity. Thus roots of $[m]_{q^v}[n]_{(q^m)^v}$ are all nmv-roots of unity that are not v-roots of unity. Similarly, roots of $[n]_{q^v}[m]_{(q^n)^v}$ are also all nmv-roots of unity that are not v-roots of unity. Since both polynomials $[m]_{q^v}[n]_{(q^m)^v}$ and $[n]_{q^v}[m]_{(q^n)^v}$ are monic,

$$[m]_{q^v}[n]_{(q^m)^v} = \frac{q^{mnv}-1}{q^v-1} = [n]_{q^v}[m]_{(q^n)^v}.$$

As $v = \max_j\{c_j\} = \max_i\{a_i\}$, it can be verified from above that A is the number of times the factor $[m]_{q^v}[n]_{(q^m)^v}$ occurs on the LHS as well as the number of times the factor $[n]_{q^v}[m]_{(q^n)^v}$ appears on the

RHS. Next we divide both sides of the equality $(*)$ by $([n]_{q^v}[m]_{(q^n)^v})^A$. This process can be repeated until both sides of $(*)$ become trivial.

Therefore, $\{c_j, d_j\}_j$ belongs to the equivalent class $\|\{a_i, b_i\}_i\|$ of $\{a_i, b_i\}_i$. As a consequence of the proof of (2), $f_n(q)$ can be generated in this fashion with respect to $\{a_i, b_i\}_i$, which contradicts to our assumption. Therefore the result follows and the proof of Part 1 is complete.

Part 2. The field of coefficients of Γ strictly contains $\mathbb{Q}$ as its prime subfield.

For this part, our main goal is to prove that there is no sequence of polynomials Γ with field of coefficients strictly contains $\mathbb{Q}$ satisfying the full hypothesis of Theorem 2.1, namely satisfying Functional Equation (2) and the condition $\deg f_n(q) = t_\Gamma(n-1)$ for all n in $\mathbb{N}$ where $t_\Gamma \geqslant 1$ is a positive number, then the same conclusion as in Part 1 holds. The above hypothesis means that the set of primes P associated to the support of Γ must contain all primes and $f_n(q)$ is nonconstant for all $n \in \mathbb{N}$. As a result, if Γ is a sequence of polynomials with field of coefficients of characteristic zero satisfying Functional Equation (2) and the condition $\deg f_n(q) = t_\Gamma(n-1)$ for all n in $\mathbb{N}$, then the field of coefficients of Γ must be $\mathbb{Q}$. Therefore, it belongs to the case of Part 1 and thus the solution of Problem 1 follows for the case of characteristic zero field of coefficients.

In this paper as well as in our next paper in this series, we will show that if the support of Γ does not strictly satisfy the above condition, then there exist sequences of polynomials Γ with coefficients not properly contained in $\mathbb{Q}$, which mean the main conclusion of Theorem 2.1 fails, i.e. at least one polynomial in this sequence cannot be written in the form $\prod_i ([n]_{a_i})^{b_i}$. Furthermore, we will establish and prove a relationship between sequences Γ with field of coefficients equal to $\mathbb{Q}$ and those with fields of coefficients strictly containing $\mathbb{Q}$ in our next paper. This allows us to classify all sequences of polynomials satisfying Functional Equation (2) whose fields of coefficients are of characteristic 0.

The essential feature that distinguishes this part from Part 1 is that, in $K[q]$ where K is any field strictly containing $\mathbb{Q}$, we do not automatically have the irreducibility of the cyclotomic polynomials. This poses the following difficulty: Let α be a root of $f_p(q)$ of order, say $r = \prod_{i=1}^{s} p_i^{l_i}$, and $m_\alpha(q)$ be its minimal polynomial over K. Then as before $m_\alpha(q)$ must divide

$$\frac{((q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}})^{p_s-1} + \cdots + (q^{\prod_{j=1}^{s-1} p_j^{l_j} p_s^{l_s-1}}) + 1)}{\prod_{a\in\mathcal{A}} P_a(q)}. \tag{3.1}$$

However $m_\alpha(q)$ is not necessarily equal to the latter product in this case. As we have seen in Part 1, the irreducibility of the cyclotomic polynomials in $\mathbb{Q}[q]$ coupled with the condition $\deg(f_p(q)) = t_\Gamma(p-1)$ for at least two primes is sufficient to ensure an affirmative answer to Problem 1. As we will see later, the full assumption that $\deg(f_n(q)) = t_\Gamma(n-1)$ for all $n \in \mathbb{N}$ (which is equivalent to the condition that P, the set of primes associated with the support of Γ, contains all prime numbers) is necessary for an affirmative answer to Problem 1.

In short, our main objective in this part is to establish the following statements:

(a) *There exists a counter-example to Theorem* 2.1 *if the hypothesis* $\deg(f_n(q)) = t_\Gamma(n-1)$ *for all* $n \in \mathbb{N}$ *is not satisfied.*
(b) *If we assume the full hypothesis of Theorem* 2.1, *in particular the condition* $\deg(f_n(q)) = t_\Gamma(n-1)$ *for all* $n \in \mathbb{N}$, *then Theorem* 2.1 *holds for this case.*

Proposition 3.11 *(Key Proposition 1). Let p and r be two distinct prime numbers, $P_{u,p}(q)$ and $P_{u,r}(q)$ be the cyclotomic polynomials in $\mathbb{Q}[q]$ of order pu and ru respectively for some positive integer $u \geqslant 1$. Let p^* and r^* be the primitive residue classes modulo u corresponding to p and r respectively. Then there exist polynomials $P'_{u,p}(q) \neq 1$ and $P'_{u,r}(q) \neq 1$ satisfying Functional Equation* (1) *and properly dividing, in the ring $\mathbb{C}[q]$, $P_{u,p}(q)$ and $P_{u,r}(q)$ respectively if and only if $u > 2$ and there exists a nonempty proper subset $\mathcal{A}$ of $(\mathbb{Z}/u\mathbb{Z})^*$ such that*

$$p\mathcal{A} = \mathcal{A}$$

and

$$r\mathcal{A} = \mathcal{A}.$$

In particular, $P'_{u,p}(q)$ and $P'_{u,r}(q)$ exist if $u > 2$ and

$$p \equiv 1 \equiv r \pmod{u}.$$

Proof. If $u = 1$, then $P_{u,p}(q)$ and $P_{u,r}(q)$ are of the form $[p]_q$ and $[r]_q$ respectively. When these polynomials are viewed in $\mathbb{C}[q]$, their roots are primitive p and r roots of unity which can be written as two collections $\{e^{\frac{2\pi is}{p}} \mid s = 1, \ldots, p-1\}$ and $\{e^{\frac{2\pi it}{p}} \mid t = 1, \ldots, r-1\}$ respectively. Suppose that there exist polynomials $P'_{u,p}(q)$ and $P'_{u,r}(q)$ satisfying Functional Equation (1) and dividing, in the ring $\mathbb{C}[q]$, $P_{u,p}(q)$ and $P_{u,r}(q)$.

Lemma 3.12. *Let $P'_{u,p}(q)$ and $P'_{u,r}(q)$ be as above. Then $P'_{u,p}(q)$ properly divides $P_{u,p}(q)$ if and only if $P'_{u,r}(q)$ properly divides $P_{u,r}(q)$. Consequently $P'_{u,p}(q)$ is in $\mathbb{Q}[q]$ if and only if $P'_{u,r}(q)$ is in $\mathbb{Q}[q]$. In particular, $P'_{1,p}(q) = [p]_q$ if and only if $P'_{1,r}(q) = [r]_q$.*

Proof. Let us suppose the contrary, say $P'_{u,p}(q)$ properly divides $P_{u,p}(q)$ but $P'_{u,r}(q)$ is $P_{u,r}(q)$. Then there exists a primitive up-root of unity α', hence a root of $P_{u,p}(q)$, which is not a root of $P'_{u,p}(q)$. Since $P'_{u,p}(q)$ and $P'_{u,r}(q) = P_{u,r}(q)$ satisfy Functional Equation (1), we obtain

$$P'_{u,p}(q)P_{u,r}\big(q^p\big) = P_{u,r}(q)P'_{u,p}\big(q^r\big).$$

The LHS contains all primitive upr-roots of unity, namely roots (not all) of $P_{u,r}(q^p)$. On the other hand, it can be verified that there exists at least one r-root of α', say α'', which is a primitive upr-root of unity. Then α'' is not a root of the RHS since otherwise α' would be a root of $P'_{u,p}(q)$. This is a contradiction. Moreover, the coefficients of $P'_{u,p}(q)$ are not properly contained in $\mathbb{Q}$ since $P_{u,p}(q)$ is irreducible in $\mathbb{Q}[q]$. Thus the result follows. □

Suppose that there exist polynomials $P'_{1,p}(q)$ and $P'_{1,r}(q)$ satisfying the conclusion of Key Proposition 1. Let us consider Functional Equation (1) with respect to $P'_{1,p}(q)$ and $P'_{1,r}(q)$:

$$P'_{1,p}(q)P'_{1,r}\big(q^p\big) = P'_{1,r}(q)P'_{1,p}\big(q^r\big). \tag{3.2}$$

Let α be a root of $P_{1,p}(q)$ which is not a root of $P'_{1,p}(q)$. Then it is a primitive p-root of unity and thus can be written as $\alpha = e^{\frac{2\pi ig}{p}}$ for some integers $1 \leqslant g \leqslant p-1$. On the LHS of (3.2), roots of $P'_{1,r}(q^p)$ are all p-roots of each root of $P'_{1,r}(q)$. Thus if $\mu = e^{\frac{2\pi il}{r}}$ is a root of $P'_{1,r}(q)$ for some $1 \leqslant l \leqslant r-1$, then every element of the set $S_\mu = \{e^{\frac{2\pi i(l+sr)}{rp}} \mid 0 \leqslant s \leqslant p-1\}$ is a root of $P_{1,r}(q^p)$. On the RHS of (3.2), roots of $P'_{1,p}(q^r)$ are all r-roots of each root of $P'_{1,p}(q)$. Since $\alpha = e^{\frac{2\pi ig}{p}}$ is not a root of $P'_{1,p}(q)$, none of the elements of the set $S_\alpha = \{e^{\frac{2\pi i(g+tp)}{pr}} \mid 0 \leqslant t \leqslant r-1\}$ is a root of $P'_{1,p}(q^r)$. Moreover, as $g + tp$ is congruent to g modulo p, none of the elements of S_α is an r-root of unity, and thus S_α contains none of the roots of $P'_{1,r}(q)$. As r and p are two distinct primes, all the elements of the collection $\mathcal{T} := \{sr \mid s = 0, \ldots, p-1\}$ are distinct modulo p, and hence we may rewrite this collection as $\mathcal{T} = \{0, \ldots, p-1\}$. Thus there exists one element, say z, in $\mathcal{T}$ such that $l + z \equiv g \pmod{p}$. Let kr be the element of $\mathcal{T}$ corresponding to z. Then $e^{\frac{2\pi i(l+kr)}{rp}} \in S_\alpha \cap S_\mu$. Therefore, $e^{\frac{2\pi i(l+kr)}{rp}}$ is not a root of the RHS of (3.2) but is a root of the LHS of (3.2) which is a contradiction. Therefore, the polynomials $P'_{1,p}(q)$ and $P'_{1,r}(q)$ satisfying the required conditions of Key Proposition 1 do not exist in this case.

Let us suppose $u > 1$. If either p or r divides u, then $P_{u,p}(q)$ and $P_{u,r}(q)$ do not satisfy Functional Equation (1). Suppose there exist polynomials $P'_{u,p}(q)$ and $P'_{u,r}(q)$ satisfying the hypothesis of Key Proposition 1. The set of roots of $P'_{u,r}(q)$ is then a proper subset A'_r of the set of roots A_r of $P_{u,r}(q)$, namely $\{e^{\frac{2\pi ic}{ru}} \mid 1 \leqslant c \leqslant ru-1,\ (c,ru)=1\}$, and thus the set of roots of $P'_{u,r}(q^p)$ is a proper subset A'_{rp} of the set $A_{rp} = \{e^{\frac{2\pi i(c+s(ru))}{(ru)p}} \mid 1 \leqslant c \leqslant ru-1,\ (c,ru)=1,\ s=0,\dots,p-1\}$, the set of all roots of $P_{u,r}(q^p)$. Similarly, the set of roots of $P'_{u,p}(q)$ is a proper subset B'_p of the set of roots B_p of $P_{u,p}(q)$ which is $\{e^{\frac{2\pi id}{pu}} \mid 1 \leqslant d \leqslant pu-1,\ (d,pu)=1\}$, and the set of roots of $P'_{u,p}(q^r)$ is a subset B'_{pr} of the set $B_{pr} = \{e^{\frac{2\pi i(d+t(pu))}{(pu)r}} \mid 1 \leqslant d \leqslant pu-1,\ (d,pu)=1,\ t=0,\dots,r-1\}$. Now notice that if p (respectively r) divide u, then $(c,ru)=1$ if and only if $(c+s(ru), rup)=1$ for $0 \leqslant s \leqslant p-1$ (resp. $(ds,pu)=1$ if and only if $(d+t(pu), pur)=1$ for $0 \leqslant t \leqslant r-1$). Therefore if p (resp. r) divides u, any p-root of a primitive ru-root of unity is a primitive rup-root of unity (respectively any r-root of a primitive pu-root of unity is a primitive pur-root of unity). On the other hand, if p (respectively r) does not divide u, then $s(ru)$ is distinct modulo p for each $s=0,\dots,p-1$ (resp. $t(pu)$ is distinct modulo r for each t in $\{0,\dots,r-1\}$). Therefore, for each c such that $1 \leqslant c \leqslant ru-1$ and $(c,ru)=1$ (resp. for each d such that $1 \leqslant d \leqslant pu-1$ and $(d,pa)=1$), there exists a unique $0 \leqslant s_c \leqslant p-1$ (resp. a unique $0 \leqslant t_d \leqslant r-1$) such that p divides $c+s_c(ra)$ (resp. r divides $d+t_d(pa)$). Thus $e^{\frac{2\pi i(c+s_c(ru))}{(ru)p}}$ and $e^{\frac{2\pi i(d+t_d(pu))}{(pu)r}}$ are primitive ru and pu-roots of unity respectively. If c_1 and c_2 are two integers which are distinct modulo ru such that $1 \leqslant c_1, c_2 \leqslant ru-1$ and $(c_1,ru)=1$ as well as $(c_2,ru)=1$, then $c_1+s_{c_1}(ru) \neq c_2+s_{c_2}(ru)$ modulo ru and thus $e^{\frac{2\pi i(c_1+s_{c_1}(ru))}{(ru)p}} \neq e^{\frac{2\pi i(c_2+s_{c_2}(ru))}{(ru)p}}$. Similarly if d_1 and d_2 are two integers which are distinct modulo pu such that $1 \leqslant d_1, d_2 \leqslant pu-1$ and $(d_1,pu)=1$ as well as $(d_2,pu)=1$, then $d_1+t_{d_1}(pu) \neq d_2+t_{d_2}(pu)$ modulo pu and thus $e^{\frac{2\pi i(d_1+t_{d_1}(pu))}{(pu)r}} \neq e^{\frac{2\pi i(d_2+t_{d_2}(pu))}{(pu)r}}$.

All of the above information can be summarized as follows:

$$P'_{u,p}\big(q^r\big) = \begin{cases} Q'_{u,p}(q)P'_{ur,p}(q) & \text{if } r \text{ does not divide } u, \\ P'_{ur,p}(q) & \text{otherwise,} \end{cases}$$

$$P'_{u,r}\big(q^p\big) = \begin{cases} Q'_{u,r}(q)P'_{up,r}(q) & \text{if } p \text{ does not divide } u, \\ P'_{up,r}(q) & \text{otherwise,} \end{cases}$$

where

- $P'_{ur,p}(q)$ is the polynomial whose roots are all distinct primitive urp-roots of unity such that when raised to r power each of them is a root of $P'_{u,p}(q)$.
- $P'_{up,r}(q)$ is the polynomial whose roots are all distinct primitive urp-roots of unity such that when raised to p power each of them is a root of $P'_{u,r}(q)$.
- $Q'_{u,p}(q)$ is some polynomial of degree equal to that of $P'_{u,p}(q)$ such that all of its roots are distinct primitive up-roots of unity.
- $Q'_{u,r}(q)$ is some polynomial of degree equal to that of $P'_{u,r}(q)$ such that all of its roots are distinct primitive ur-roots of unity.

From our assumption that $P'_{u,p}$ and $P'_{u,r}(q)$ satisfy Functional Equation (1), we have

$$P'_{u,p}(q)P'_{u,r}\big(q^p\big) = P'_{u,r}(q)P'_{u,p}\big(q^r\big)$$

which is then equivalent to

$$P'_{u,p}(q)P'_{up,r}(q) = P'_{u,r}(q)Q'_{u,p}(q)P'_{ur,p}(q)$$

if r divides u but p does not; and is equivalent to

$$P'_{u,p}(q)Q'_{u,r}(q)P'_{up,r}(q) = P'_{u,r}(q)P'_{ur,p}(q)$$

if p divides u but r does not; and is equivalent to

$$P'_{u,p}(q)P'_{up,r}(q) = P'_{u,r}(q)P'_{ur,p}(q)$$

if pr divides u. For the last three equations to be true, it is necessary for $P'_{up,r}(q)$ to be equal to $P'_{ur,p}(q)$ since they are the only factors on each side of these equations whose roots are primitive upr-roots of unity. However, when this is true, the equalities in each of these equations do not hold. That contradicts our assumption. Therefore the desired polynomials do not exist in these cases.

If pr does not divide u, then Functional Equation (1) of $P'_{u,p}(q)$ and $P'_{u,r}(q)$ must have the form

$$P'_{u,p}(q)Q'_{u,r}(q)P'_{up,r}(q) = P'_{u,r}(q)Q'_{u,p}(q)P'_{ur,p}(q)$$

where the equality can only hold if $P'_{up,r}(q) = P'_{ur,p}(q)$, $P'_{u,p}(q) = Q'_{u,p}(q)$, and $P'_{u,r}(q) = Q'_{u,r}(q)$.

Let $u = \prod_j p_j^{h_j}$ be the prime factorization of u. As $P'_{u,p}(q)$ properly divides $P_{u,p}(q)$, there exists at least one root α which is a root of the latter but not the former. If we write $\alpha = e^{\frac{2\pi id}{up}}$ for some integer d in $\{1,\dots,up-1\}$ with $(d,up)=1$, then none of the elements of the collection $\mathcal{P} = \{e^{\frac{2\pi i(d+t(up))}{(up)r}} \mid t = 0,\dots,r-1\}$, the set of all r-roots of α, is a root of $P'_{u,p}(q^r)$. By the Chinese Remainder Theorem (CRT), d is uniquely determined by a tuple of integers $(d_p, \{d_{p_j}\}_j)$ where $d_p \in \{1,\dots,p-1\}$ and $d_{p_j} \in (\mathbb{Z}/(p_j)^{h_j}\mathbb{Z})^*$ for each p_j dividing u.

Remark 3.13. From now on, whenever necessary and appropriate we identify a root of unity, say $e^{2\pi iw/(\prod_j p_j^{h_j})}$, which is uniquely determined by [w], the residue class of w modulo $\prod_j p_j^{h_j}$, with $[w]$ or, if appropriate, with the tuple of integers $(w_{p_j})_j$ via the Chinese Remainder Theorem where w_{p_j} denotes the residue class of w modulo $p_j^{h_j}$.

Lemma 3.14. *All the roots of $P_{u,p}(q)$ of the form $e^{\frac{2\pi iw}{up}}$ where w is equivalent, via CRT, to the tuple of the form $(w_p, \{w_{p_j}\}_j)$ with w_p in $\{1,\dots,p-1\}$ different from d_p and $w_{p_j} = d_{p_j}$ for all j must* **Not** *be roots of $P'_{u,p}(q)$. In other words, for each primitive residue class d modulo u represented by a tuple $(d_{p_j})_j$, all the roots of $P_{u,p}(q)$ of the form $e^{\frac{2\pi iw}{up}}$ with $w \overset{(CRT)}{\longleftrightarrow} w_p \times (d_{p_j})_j$ and $w_p \in \{1,\dots,p-1\}$ are either all roots of $P_{u,p}(q)$ or none is.*

Proof. Let us suppose the contrary. Let $e^{\frac{2\pi iw}{up}}$ be one such root which is a root of $P'_{u,p}(q)$. As $e^{\frac{2\pi iw}{up}}$ is determined uniquely by w, we represent this root by w. Then $e^{\frac{2\pi i(w+t(up))}{(up)r}}$ is a root of $P'_{u,p}(q^r)$ for $0 \leqslant t \leqslant r-1$. For Functional Equation (1) to hold, $e^{\frac{2\pi i(w+t(up))}{(up)r}}$ must also be a root of $P'_{u,r}(q^p)$ for $0 \leqslant t \leqslant r-1$ such that $(w+t(up), upr) = 1$. Now roots of $P'_{u,r}(q)$ are of the form $e^{\frac{2\pi ic}{ur}}$ for integers $1 \leqslant c \leqslant ur-1$ with $(c,ur)=1$ and thus all the roots of $P'_{u,r}(q^p)$ must be the collection $\mathcal{R} = \{e^{\frac{2\pi i(c+s(ur))}{(ur)p}} \mid s = 0,\dots,p-1,\ 1 \leqslant c \leqslant ur-1,\ (c,ur)=1\}$ where $e^{\frac{2\pi ic}{ur}}$ is a root of $P'_{u,r}(q)$. Thus there exist some integer c_1 with $1 \leqslant c_1 \leqslant ur-1$, $(c_1,ur)=1$ and $s_1 \in \{0,\dots,p-1\}$ such that $e^{\frac{2\pi i(w+t_1(up))}{(up)r}} = e^{\frac{2\pi i(c_1+s_1(ur))}{(ur)p}} \in \mathcal{R}$ for some integer t_1 in $\{0,\dots,r-1\}$ with $(w+t_1(up), upr) = 1$. Thus $c_1 \equiv w \equiv d \pmod{u}$. Therefore, each element of the collection $\{e^{\frac{2\pi i(c_1+s(ur))}{(ur)p}} \mid s = 0,\dots,p-1\}$ is a root of $P'_{u,r}(q^p)$. Now as $(ur,p)=1$,

all the elements of the collection $\{s(ur) \mid s = 0, \ldots, p-1\}$ are distinct modulo p. Hence there exists a unique integer s_2 such that $c_1 + s_2(ur) \equiv d(\text{modulo } p)$ and is thus congruent to d modulo up as $c_1 \equiv d \pmod{u}$ and $(u, p) = 1$. Similarly, as t varies between 0 and $r-1$, there exists an integer, say t_1, such that $d + t_1(up)$ is congruent to $c_1 + s_2(ur)$ modulo r. Therefore, $d + t_1(up)$ is congruent to $c_1 + s_2(ur)$ modulo r, p, u and thus $e^{\frac{2\pi i(c_1+s_2(ur))}{(ur)p}}$ must be in $\mathcal{P}$. This is a contradiction and the lemma is proved. □

Lemma 3.15. *Let $P'_{u,p}(q)$ and $P'_{u,r}(q)$ be as in the statement of Key Proposition* 1. *Then $P'_{up,r}(q) = P'_{ur,p}(q)$, $P'_{u,p}(q) = Q'_{u,p}(q)$, and $P'_{u,r}(q) = Q'_{u,r}(q)$ hold if and only if the following statements hold*:

(1) *The collection of all roots of $P'_{u,p}(q)$ and $P'_{u,r}(q)$ are represented by*

$$\left\{(\kappa_p, \nu_p) \;\middle|\; \kappa_p \in \mathcal{A},\ \nu_p \in (\mathbb{Z}/p\mathbb{Z})^*\right\}$$

and

$$\left\{(\kappa_r, \nu_r) \;\middle|\; \kappa_r \in \mathcal{A},\ \nu_r \in (\mathbb{Z}/r\mathbb{Z})^*\right\}$$

respectively where $\mathcal{A}$ is any proper subset of $(\mathbb{Z}/u\mathbb{Z})^*$.

(2) *$p\mathcal{A} = \mathcal{A}$ and $r\mathcal{A} = \mathcal{A}$.*

In particular, (1) *and* (2) *are satisfied if $u > 2$ and the residues classes p^* and r^* are both congruent to* 1 *modulo u.*

Proof. Let c be an integer such that $1 \leqslant c \leqslant ru - 1$ and $(c, ru) = 1$. Suppose that $e^{\frac{2\pi ic}{ru}}$ is a root of $P'_{u,r}(q)$. Then $e^{\frac{2\pi i(c+s_c(ru))}{(ru)p}}$, where $0 \leqslant s_c \leqslant p-1$ is defined as above, is a root of $P'_{u,r}(q^p)$. Let c' denote the integer $\frac{c+s_c(ru)}{p}$. Then $c' \equiv p^{-1}c$ modulo ru, or equivalently, $pc' \equiv c$ modulo ru. Then the root of $Q'_{u,r}(q)$ represented by $[\frac{c+s_c(ru)}{p}]$ is a translation by p^{-1} of a root of $P'_{u,r}(q)$ represented by $[c]$ in the group $(\mathbb{Z}/ru\mathbb{Z})^* \cong (\mathbb{Z}/u\mathbb{Z})^* \times (\mathbb{Z}/r\mathbb{Z})^*$. Therefore, every root of $Q'_{u,r}(q)$, viewed as an element of the group $(\mathbb{Z}/ru\mathbb{Z})^*$, is a translation of a root $P'_{u,r}(q)$ viewed as an element in the group $(\mathbb{Z}/ru\mathbb{Z})^*$ by p^{-1}. Similarly, every root of $Q'_{u,p}(q)$, viewed as an element of the group $(\mathbb{Z}/pu\mathbb{Z})^* \cong (\mathbb{Z}/u\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$, is a translation of a root $P'_{u,p}(q)$ viewed as an element in the group $(\mathbb{Z}/pu\mathbb{Z})^*$ by r^{-1}. By Lemma 3.14, the collection of roots of $P'_{u,p}(q)$ and $P'_{u,r}(q)$ can be represented by $\{(\kappa_p, \nu_p) \mid \kappa_p \in A_p,\ \ \nu_p \in (\mathbb{Z}/p\mathbb{Z})^*\}$ and $\{(\kappa_r, \nu_r) \mid \kappa_r \in A_r,\ \ \nu_r \in (\mathbb{Z}/r\mathbb{Z})^*\}$ respectively where A_p and A_r are two proper subsets of $(\mathbb{Z}/u\mathbb{Z})^*$. As a result, roots of $P'_{up,r}(q)$ and $P'_{ur,p}(q)$ can be represented by the collections $\{(\kappa_r, \nu_r, \nu_p) \mid \kappa_r \in A_r,\ \ \nu_r \in (\mathbb{Z}/r\mathbb{Z})^*,\ \ \nu_p \in (\mathbb{Z}/p\mathbb{Z})^*\}$ and $\{(\kappa_p, \nu_p, \nu_r) \mid \kappa_p \in A_p,\ \ \nu_p \in (\mathbb{Z}/p\mathbb{Z})^*,\ \ \nu_r \in (\mathbb{Z}/r\mathbb{Z})^*\}$ respectively. This means that $P'_{up,r}(q) = P'_{ur,p}(q)$ if and only if $A_r = A_p$. Let $\mathcal{A}$ denote both A_p and A_r. Now $(\mathbb{Z}/u\mathbb{Z})^*$ has at least one nonempty proper subgroup if and only if $u > 2$. Since p does not divide ur and r does not divide up by assumption, $(p, ur) = (r, up) = 1$. Therefore, $P'_{u,p}(q) = Q'_{u,p}(q)$, and $P'_{u,r}(q) = Q'_{u,r}(q)$ if any only if $p\mathcal{A} = r\mathcal{A} = \mathcal{A}$. In particular, $P'_{u,p}(q) = Q'_{u,p}(q)$, and $P'_{u,r}(q) = Q'_{u,r}(q)$ if $p^* = 1 = r^*$ where p^* and r^* are the residue classes of p and r modulo u respectively. Thus the result follows. □

Lemma 3.15 implies that there exist polynomials $P'_{u,p}(q)$ and $P'_{u,r}(q)$ properly dividing $P_{u,p}(q)$ and $P_{u,r}(q)$ respectively which satisfy Functional Equation (1).

Let us construct the polynomials $P'_{u,p}(q)$ and $P'_{u,r}(q)$ above from $P_{u,p}(q)$ and $P_{u,r}(q)$ respectively. Let $P_p(q)$ and $P_r(q)$ be two polynomials properly dividing $P_{u,p}(q)$ and $P_{u,r}(q)$ respectively such that their roots can be represented by two collections of tuples $\{(\kappa, \nu_p) \mid \kappa \in (\mathbb{Z}/u\mathbb{Z})^* - \mathcal{A},\ \ \nu_p \in (\mathbb{Z}/p\mathbb{Z})^*\}$ and $\{(\kappa, \nu_r) \mid \kappa \in (\mathbb{Z}/u\mathbb{Z})^* - \mathcal{A},\ \ \nu_r \in (\mathbb{Z}/r\mathbb{Z})^*\}$ respectively. If we define: $P'_{u,p}(q) := P_{u,p}(q)/P_p(q)$ and $P'_{u,r}(q) := P_{u,r}(q)/P_r(q)$ respectively, then $P'_{u,p}(q)$ and $P'_{u,r}(q)$ satisfy Functional Equation (1)

by Lemma 3.15. Note that the coefficients of $P'_{u,p}(q)$ and $P'_{u,r}(q)$ are not properly contained in $\mathbb{Q}$ and thus cannot be written as products of quantum integers. The proof of Key Proposition 1 is thus complete. □

Remark 3.16. Key Proposition 1 allows us to produce sequences of polynomials Γ's, with field of coefficients of characteristic zero strictly containing $\mathbb{Q}$, which satisfies Functional Equation (2), where the set P associated to the support A_P of Γ is of large cardinality. This is shown in [5]. The elements of such sequences are not necessarily expressible in term of quantum integers as in Theorem 2.1.

Key Proposition 1 also provides another proof for Theorem 8 in [1] in the case where the fields of coefficients are of characteristic zero. This method can be generalized to the case where $t_\Gamma > 1$ while this does not seem possible with the method in the proof of Theorem 8 in [1]. However, the latter method covered fields of all characteristic for the case $t_\Gamma = 1$.

Definition 3.17. 1) Let $F_{u,p}(q)$ and $F_{u,r}(q)$ be two polynomials dividing $P_{u,p}(q)$ and $P_{u,r}(q)$ respectively. If they satisfy the condition that for each primitive residue class w modulo u, all the roots of $P_{u,p}(q)$ represented by the collection of tuples $\{(\gamma_p, (w_{p_j})_j) \mid \gamma_p = 1, \dots, p-1\}$ if p does not divide u (resp. by the collection $\{(w_p + t(p^l), (w_{p_j})_{j,p_j \neq p}) \mid t = 0, \dots, p-1\}$ if $p^l \| u$ for some positive integer $l \geqslant 1$ and where w_p is the residue class of w modulo p) are roots $F_{u,p}(q)$ if and only if all the roots of $P_{u,r}(q)$ represented by the collection $\{\gamma_r, (w_{p_j})_j \mid \gamma_r = 1, \dots, r-1\}$ if r does not divide u (resp. by the collection $\{w_r + s(r^h), (w_{p_j})_{j,p_j \neq r} \mid s = 0, \dots, r-1\}$ if $r^h \| u$ for some positive integer $h \geqslant 1$ where w_r is the residue class of w modulo r) are roots $F_{u,r}(q)$, then we say that $F_{u,p}(q)$ and $F_{u,r}(q)$ are **compatible**. For example, $P_{u,p}(q)$ and $P_{u,r}(q)$ are compatible for any positive integer u, primes p and r, a fact which was proved earlier for the case where pr does not divide u. This fact is shown later in the case when either p or r divides u.

2) The polynomials $f_{u,p}(q)$ and $f_{u,r}(q)$ are said to be **super-compatible** if $f_{u,p}(q) = \prod_i (F^{(i)}_{u,p}(q))^{n_i}$ and $f_{u,r}(q) = \prod_i (F^{(i)}_{u,r}(q))^{n_i}$ where $F^{(i)}_{u,p}(q)$ and $F^{(i)}_{u,r}(q)$ are polynomials which are compatible for all i.

For example, $P_{u,p}(q)^n$ and $P_{u,r}(q)^n$ are super-compatible for any nonnegative integer n where $P_{u,p}(q)^n$ and $P_{u,r}(q)^n$ are the cyclotomic polynomials with coefficients in $\mathbb{Q}$ of order up and ur respectively.

Remark 3.18. At this point, the above definition only makes sense in the case where pr does not divide u due to our analysis in the paragraphs above it. The other cases will be explained later. Also, the decomposition of $f_{u,\square}(q)$ into polynomials $F^{(i)}_{u,\square}(q)$'s, where $\square$ denotes either p or r, in the definition of super-compatibility may not be unique.

Let p and r be primes in the support of Γ. Let $f_{u_p,p}(q)$ be the factor of $f_p(q)$ in $\mathbb{C}[q]$ such that its roots consist of all the roots of $f_p(q)$ with multiplicities which are primitive pu_p-roots of unity. Then $f_p(q) = \prod_{u_{p,j} > u_{p,j+1}} f_{u_{p,j},p}(q)$ in the ring $\mathbb{C}[q]$. Similarly defined, we have $f_r(q) = \prod_{u_{r,i} > u_{r,i+1}} f_{u_{r,i},r}(q)$. Unless stated otherwise, we assume from this point on that each factor appearing in these products are nontrivial. We call j (resp. i) the **j-level** (resp. **i-level**) and $u_{p,j}$ (resp. $u_{r,i}$) the **value** of the j-level (resp. i-level) of $f_p(q)$ (resp. $f_r(q)$) if $f_{u_{p,j}}(q)$ (resp. $f_{u_{r,i}}(q)$) is a nontrivial factor of $f_p(q)$ (resp. $f_r(q)$). Define $V := \{v_{p,r,k} \mid v_{p,r,k} > v_{p,r,k+1}\} := \{u_{p,j}\}_j \cup \{u_{r,i}\}_i$. We refer to k as the **k-bi-level** with respect to p and r and $v_{p,r,k}$ the **value** of the k-bi-level of $f_p(q)$ and $f_r(q)$. Note that level i of $f_p(q)$ or $f_r(q)$ is not necessarily equal to the bi-level i of $f_p(q)$ and $f_r(q)$. Using V and these product decompositions, we write Functional Equation (1) with respect to $f_p(q)$ and $f_r(q)$ as:

$$
\begin{array}{ccc}
f_{v_{p,r,1},p}(q)^{s_{p,1}} f_{v_{p,r,1},r}\left(q^p\right)^{s_{r,1}} & \overset{(1)}{\longleftrightarrow} & f_{v_{p,r,1},r}(q)^{s_{r,1}} f_{v_{p,r,1},p}\left(q^r\right)^{s_{p,1}} \\
\dots & \dots & \dots \\
f_{v_{p,r,k},p}(q)^{s_{p,k}} f_{v_{p,r,k},r}\left(q^p\right)^{s_{r,k}} & \overset{(k)}{\longleftrightarrow} & f_{v_{p,r,k},r}(q)^{s_{r,k}} f_{v_{p,r,k},p}\left(q^r\right)^{s_{p,k}} \\
\dots & \dots & \dots \\
f_p(q) f_r\left(q^p\right) & = & f_r(q) f_p\left(q^r\right)
\end{array}
$$

where:

(i) $s_{p,k} = 1$ if $f_{v_{p,r,k},p}(q)$ nontrivially divides $f_p(q)$ and 0 otherwise,
(i′) $s_{r,k} = 1$ if $f_{v_{p,r,k},r}(q)$ nontrivially divides $f_r(q)$ and 0 otherwise,
(ii) $\prod_k f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}} f_{v_{p,r,k},r}(q^p)^{s_{r,k}} = f_p(q) f_r(q^p)$,
(ii′) $\prod_j f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}} f_{v_{p,r,k},p}(q^r)^{s_{p,j}} = f_r(q) f_p(q^r)$,
(iii) the symbol $\overset{(j)}{\longleftrightarrow}$ indicates the form of Functional Equation (1) at the bi-level j (note that the polynomial expressions on the left-hand side and the right-hand side of $\longleftrightarrow$ at each bi-level are not necessarily equal).

Such a version of Functional Equation (1) is called **Expanded Functional Equation** (1) with respect to p and r, denoted by EFE(1). EFE(1) above is said to be in **reduced form** (rf) if at each level k where pr does not divide $v_{p,r,k}$, the line

$$f_{v_{p,r,k},p}(q)^{s_{p,k}} f_{v_{p,r,k},r}\big(q^p\big)^{s_{r,k}} \overset{(k)}{\longleftrightarrow} f_{v_{p,r,k},r}(q)^{s_{r,k}} f_{v_{p,r,k},p}\big(q^r\big)^{s_{p,k}}$$

in EFE(1) is replaced by

(i) $f_{v_{p,r,k},r}(q^p)^{s_{r,k}} \overset{(k)}{\longleftrightarrow} f_{v_{p,r,k},r}(q)^{s_{r,k}} \frac{f_{v_{p,r,k},p}(q^r)^{s_{p,k}}}{f_{v_{p,r,k},p}(q)^{s_{p,k}}}$ if $(r, v_{p,r,k}) = 1$.
(ii) $f_{v_{p,r,k},p}(q)^{s_{p,k}} \frac{f_{v_{p,r,k},r}(q^p)^{s_{r,k}}}{f_{v_{p,r,k},r}(q)^{s_{r,k}}} \overset{(k)}{\longleftrightarrow} f_{v_{p,r,k},p}(q^r)^{s_{p,k}}$ if $(p, v_{p,r,k}) = 1$, or
(iii) $\frac{f_{v_{p,r,k},p}(q^r)^{s_{p,k}}}{f_{v_{p,r,k},p}(q)^{s_{p,k}}} \overset{(k)}{\longleftrightarrow} \frac{f_{v_{p,r,k},r}(q^p)^{s_{r,k}}}{f_{v_{p,r,k},r}(q)^{s_{r,k}}}$ if $(pr, v_{p,r,k}) = 1$,
(iv) line $f_p(q) f_r(q^p) = f_r(q) f_p(q^r)$ is replaced by $Q_{p,r}(q) = Q_{p,r}(q)$ where $Q_{p,r}(q)$ is the product of all expressions of the left-hand columns (or the right-hand column) after either (i), (ii) or (iii) has taken place, i.e.,

$$\begin{aligned} Q_{p,r}(q) &= \frac{f_p(q) f_r(q^p)}{\prod_i f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})} f_{v_{p,r,i},p}(q)^{s_{p,i}(1-\delta_{r,i})}} \\ &= \frac{f_r(q) f_p(q^r)}{\prod_i f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})} f_{v_{p,r,i},p}(q)^{s_{p,i}(1-\delta_{r,i})}}. \end{aligned}$$

If all expressions appearing in the left-hand column and the right-hand column of the reduced form of an EFE(1) can be rearranged (without factoring the individual factors) within their corresponding columns so that $\overset{(i)}{\longleftrightarrow}$ can be replaced by $\overset{(i)}{=}$ at each bi-level $i \leqslant l$, then we say that it is in **l-super-reduced form**. If $\overset{(i)}{\longleftrightarrow}$ can be replaced by $\overset{(i)}{=}$ at all bi-level i, then we say that it is in **super-reduced form**.

Some remarks are needed at this point to explain the above definitions.

Remark 3.19. (1) The product of all the rational expressions in the left-hand column and the product of those in the right-hand column of the reduced form of an EFE(1) are equal, and thus it makes sense to denote both products by the same polynomial $Q_{p,r}(q)$ as in (iv) above; (2) $Q_{p,r}(q)$ divides $f_{u_1,p}(q) f_{u_1,r}(q^p)$ and thus $f_{u_1,r}(q) f_{u_1,p}(q^r)$; (3) For each line (i), the product of all expressions on both sides of $\overset{(i)}{\longleftrightarrow}$ remains equal before and after either (i), (ii) or (iii) has taken place. It is shown below that all the rational expressions in the definition above are actually polynomials when they occur, and that for each of these rational expressions, its roots are primitive roots of unity of the same order. Also, a reduced form of an EFE(1) is automatically in super-reduced form without rearranging if and only if pr does not divide $v_{p,r,i}$ for all levels i.

Proposition 3.20 *(Key Proposition 1′).*

(i) *Let Γ be a sequence of polynomials with field of coefficients of characteristic zero. Let p and r be any two distinct primes in the support of Γ. Let $u_{p,1}$ be the first level of $f_p(q)$ and $u_{r,1}$ be the first level of $f_r(q)$. Let $v_{p,r,1}$ be the value of the first bi-level of* EFE(1) *with respect to p and r. Then*:

(1) *$v_{p,r,1}$ is equal to $u_{p,1}$ and $u_{r,1}$. As a result, $s_{c,1} = 1$ and $u_{c,1}$ is the same for all primes c in the support of Γ and thus can be unambiguously denoted by u_1.*
(2) *Let $f_{u_1,p}(q)$ be the factor of $f_p(q)$ whose roots are all the primitive $u_1 p$-roots of unity which are roots of $f_p(q)$, and let $f_{u_1,r}(q)$ be similarly defined with r replacing p. Then $f_{u_1,p}(q) = (P_{u_1,p}(q))^n$ if and only if $f_{u_1,r}(q) = (P_{u_1,r}(q))^n$ and thus $f_{u_1,p}(q)$ has coefficients in $\mathbb{Q}$ if and only if $f_{u_1,r}(q)$ does.*
(3) *$f_{u_1,p}(q)$ and $f_{u_1,r}(q)$ are super-compatible.*
(4) *All the rational expressions in the reduced form of* EFE(1)*, with respect to p and r, are polynomials.*

(ii) *Let $\square$ denote either p or r and $\triangle$ denote the other. Let $f_{u,\square}(q)$ be a monic polynomial whose roots are primitive $u\square$-roots of unity such that*:

- *Its coefficients are not properly contained in $\mathbb{Q}$.*
- *$f_{u,\square}(q)$ does not properly divide $P_{u,\square}(q)$.*

Then

$$\frac{f_{u,\square}(q^{\triangle})}{f_{u,\square}(q)}$$

is a polynomial if and only if there is a factorization

$$\frac{f_{u,\square}(q^{\triangle})}{f_{u,\square}(q)} = \prod_j \left(\frac{\pi^{(j)}_{u,\square}(q^{\triangle})}{\pi^{(j)}_{u,\square}(q)} \right)^{e_j}$$

such that $\frac{\pi^{(j)}_{u,\square}(q^{\triangle})}{\pi^{(j)}_{u,\square}(q)}$, where $\pi^{(j)}_{u,\square}(q)$ divides $P_{u,\square}(q)$, is a polynomial for each j.

Proof. (1) Let us consider the first line of EFE(1) with respect to p and r,

$$f_{v_{p,r,1},p}(q)^{s_{p,1}} f_{v_{p,r,1},r}\left(q^p\right)^{s_{r,1}} \overset{(1)}{\longleftrightarrow} f_{v_{p,r,1},r}(q)^{s_{r,1}} f_{v_{p,r,1},p}\left(q^r\right)^{s_{p,1}}$$

where either $s_{p,1} = 1$ or $s_{r,1} = 1$. Without loss of generality, we may suppose that $s_{p,1} = 1$. Thus $u_{p,1} = v_{p,r,1}$. Then from the proof of Key Proposition 1, $f_r(q) f_p(q^r)$ possesses at least one root, say α, which is a $v_{p,r,1} pr$-root of unity. As $v_{p,r,1} > v_{p,r,i}$ for any level $i > 1$, the order of α as a root of unity is maximal among all the roots of $f_r(q) f_p(q^r)$. Therefore α must also be a root of $f_p(q) f_r(q^p)$ which is of maximal order as roots of unity, namely $v_{p,r,1} pr$, among the roots of $f_r(q) f_p(q^r)$, and that is only possible if $s_{r,1} = 1$. As a result, $v_{p,r,1} = u_{r,1}$ and thus $u_{p,1} = u_{r,1}$ for any arbitrary primes p and r in the support of Γ. Therefore, $u_{c,1}$ is the same and hence $s_{c,1} = 1$ for all primes c in the support of Γ. Hence we can denote $u_{c,1}$ for any prime c in the support of Γ unambiguously as u_1.

(2) Let m_p and m_r be the greatest nonnegative integers such that $(P_{u_1,p}(q))^{m_p}$ and $(P_{u_1,r}(q))^{m_r}$ divide $f_{u_1,p}(q)$ and $f_{u_1,r}(q)$ respectively.

First we show that $m_p = m_r$ for all primes p and r in the support of Γ.

(a) Suppose that pr does not divide u_1. By the proof of Key Proposition 1,

$$\frac{(P_{u_1,r}(q^p))^{m_r}}{(P_{u_1,r}(q))^{m_r}} = \left(P_{u_1 p,r}(q)\right)^{m_r} = \left(P_{u_1 r,p}(q)\right)^{m_r} = \frac{(P_{u_1,p}(q^r))^{m_r}}{(P_{u_1,p}(q))^{m_r}}.$$

By replacing $f_{u_1,p}(q)$ by $\frac{f_{u_1,p}(q)}{P_{u_1,p}(q)^{m_p}} P_{u_1,p}(q)^{m_p}$ and $f_{u_1,r}(q)$ by $\frac{f_{u_1,r}(q)}{P_{u_1,r}(q)^{m_r}} P_{u_1,r}(q)^{m_r}$ and dividing both sides of $\overset{(1)}{\longleftrightarrow}$ by $P_{u_1,p}(q)^{m_p} P_{u_1,r}(q)^{m_r}$, line (1) of EFE(1) becomes:

$$\frac{f_{u_1,p}(q)}{P_{u_1,p}(q)^{m_p}} \frac{f_{u_1,r}(q^p)}{P_{u_1,r}(q^p)^{m_p}} \frac{P_{u_1,r}(q^p)^{m_r}}{P_{u_1,r}(q)^{m_r}} \overset{(1)}{\longleftrightarrow} \frac{f_{u_1,r}(q)}{P_{u_1,r}(q)^{m_r}} \frac{f_{u_1,p}(q^r)}{P_{u_1,p}(q^r)^{m_p}} \frac{P_{u_1,p}(q^r)^{m_p}}{P_{u_1,p}(q)^{m_p}},$$

which is equivalent to

$$\frac{f_{u_1,p}(q)}{P_{u_1,p}(q)^{m_p}} \frac{f_{u_1,r}(q^p)}{P_{u_1,r}(q^p)^{m_p}} \big(P_{u_1p,r}(q)\big)^{m_r} \overset{(1)}{\longleftrightarrow} \frac{f_{u_1,r}(q)}{P_{u_1,r}(q)^{m_r}} \frac{f_{u_1,p}(q^r)}{P_{u_1,p}(q^r)^{m_p}} \big(P_{u_1r,p}(q)\big)^{m_p}.$$

Thus m_r is the highest power of $P_{u_1p,r}(q)$ dividing $f_{u_1,p}(q) f_{u_1,r}(q^p)$ and m_p is the highest power of $P_{u_1r,p}(q)$ dividing $f_{u_1,r}(q) f_{u_1,p}(q^r)$. Therefore $m_p = m_r$ in this case.

(b) Suppose either p or r divides u_1. By symmetry, we only need to consider two cases: (i) r divides u_1 and p does not; (ii) pr divides u_1.

(i) By the proof of Key Proposition 1,

$$\frac{P_{u_1,r}(q^p)^{m_r}}{P_{u_1,r}(q)^{m_r}} = P_{u_1p,r}(q)^{m_r} = P_{u_1,p}\big(q^r\big)^{m_r}.$$

For this case, we again replace $f_{u_1,p}(q)$ and $f_{u_1,r}(q)$ by $\frac{f_{u_1,p}(q)}{P_{u_1,p}(q)^{m_p}} P_{u_1,p}(q)^{m_p}$ and $\frac{f_{u_1,r}(q)}{P_{u_1,r}(q)^{m_r}} P_{u_1,r}(q)^{m_r}$ respectively and divide both sides of line (1) by $P_{u_1,r}(q)^{m_r}$. Then line (1) of EFE(1) becomes

$$f_{u_1,p}(q) \frac{f_{u_1,r}(q^p)}{P_{u_1,r}(q^p)^{m_p}} \frac{P_{u_1,r}(q^p)^{m_r}}{P_{u_1,r}(q)^{m_r}} \overset{(1)}{\longleftrightarrow} \frac{f_{u_1,r}(q)}{P_{u_1,r}(q)^{m_r}} \frac{f_{u_1,p}(q^r)}{P_{u_1,p}(q^r)^{m_p}} P_{u_1,p}\big(q^r\big)^{m_p},$$

which is equivalent to

$$f_{u_1,p}(q) \frac{f_{u_1,r}(q^p)}{P_{u_1,r}(q^p)^{m_p}} \big(P_{u_1p,r}(q)\big)^{m_r} \overset{(1)}{\longleftrightarrow} \frac{f_{u_1,r}(q)}{P_{u_1,r}(q)^{m_r}} \frac{f_{u_1,p}(q^r)}{P_{u_1,p}(q^r)^{m_p}} \big(P_{u_1r,p}(q)\big)^{m_p}.$$

By the same reasoning as in part (a), we also have $m_p = m_r$.

(ii) By the proof of Key Proposition 1, if pr divides u_1 then

$$P_{u_1,r}\big(q^p\big)^{m_r} = P_{u_1p,r}(q)^{m_r} = P_{u_1r,p}(q)^{m_r} = P_{u_1,p}\big(q^r\big)^{m_r}$$

and

$$P_{u_1,p}\big(q^r\big)^{m_p} = P_{u_1r,p}(q)^{m_p} = P_{u_1p,r}(q)^{m_p} = P_{u_1,r}\big(q^p\big)^{m_p}.$$

Let us replace $f_{u_1,p}(q)$ and $f_{u_1,r}(q)$ by $\frac{f_{u_1,p}(q)}{P_{u_1,p}(q)^{m_p}} P_{u_1,p}(q)^{m_p}$ and $\frac{f_{u_1,r}(q)}{P_{u_1,r}(q)^{m_r}} P_{u_1,r}(q)^{m_r}$ respectively. Then line (1) of the reduced form of EFE(1) with respect to p and r becomes:

$$f_{u_1,p}(q) \frac{f_{u_1,r}(q^p)}{P_{u_1,r}(q^p)^{m_r}} P_{u_1,r}\big(q^p\big)^{m_r} = f_{u_1,r}(q) \frac{f_{u_1,p}(q^r)}{P_{u_1,p}(q^r)^{m_p}} P_{u_1,p}\big(q^r\big)^{m_p},$$

which is equivalent to

$$f_{u_1,p}(q)\frac{f_{u_1,r}(q^p)}{P_{u_1,r}(q^p)^{m_r}}P_{u_1p,r}(q)^{m_r} = f_{u_1,r}(q)\frac{f_{u_1,p}(q^r)}{P_{u_1,p}(q^r)^{m_p}}P_{u_1r,p}(q)^{m_p}.$$

Again by the same reasoning as in part (a), we also have $m_p = m_r$ in this case.

Therefore there is a nonnegative number m such that $m_p = m_r = m$ for all primes p and r in the support of Γ. If $f_{u_1,p}(q) = P^m_{u_1,p}(q)$, then $P^m_{u_1,r}(q)$ divides $f_{u_1,r}(q)$. If $P^m_{u_1,p}(q)$ properly divides $f_{u_1,r}(q)$, then by a counting argument, it can be verified that $f_{u_1,p}(q)f_{u_1,r}(q^p)$ possesses more primitive u_1pr-roots of unity than $f_{u_1,r}(q)f_{u_1,p}(q^r)$. Therefore, $f_{u,p}(q)f_{u,r}(q^p)$ contains more primitive u_1pr-roots of unity than $f_{u,r}(q)f_{u,p}(q^r)$, which contradicts Functional Equation (1). Thus $f_{u_1,r}(q) = P^m_{u_1,r}(q)$. By symmetry, if $f_{u_1,r}(q) = P^m_{u_1,r}(q)$, then $f_{u_1,p}(q) = P^m_{u_1,p}(q)$. As a result, (2) follows.

(3) To prove this part, we first need to prove the analogue of Lemma 3.14 in the case where either p or r divides $u = u_1$. This explains the definition of compatible and super-compatible for these cases stated earlier. By (2), $f_{u_1,p}(q)$ and $f_{u_1,r}(q)$ are super-compatible if and only if $\frac{f_{u_1,p}(q)}{P_{u_1,p}(q)^m}$ and $\frac{f_{u_1,r}(q)}{P_{u_1,r}(q)^m}$ are super-compatible. To prove (3) we may assume that $f_{u_1,p}(q)$ and $f_{u_1,r}(q)$ are nontrivial and $m = 0$ since otherwise, we can replace $f_{u_1,p}(q)$ and $f_{u_1,r}(q)$ by $\frac{f_{u_1,p}(q)}{P_{u_1,p}(q)^m}$ and $\frac{f_{u_1,r}(q)}{P_{u_1,r}(q)^m}$ respectively. Suppose that either p or r divides u_1. By symmetry, there are only two cases to consider: (a) p does not divide u_1 and r does; (b) pr divides u_1.

(a) Let us suppose that r divides u_1 and p does not: We examine the relationship between the roots of the corresponding factors $f_{u_1,p}(q)$ and $f_{u_1,r}(q)$. Let $1 \leqslant b \leqslant u_1p - 1$ and $1 \leqslant c \leqslant u_1r - 1$ be two positive integers such that $e^{\frac{2\pi ib}{u_1p}}$ and $e^{\frac{2\pi ic}{u_1r}}$ are roots of $f_{u_1,p}(q)$ and $f_{u_1,r}(q)$ respectively. Hence $(b, u_1p) = 1$ and $(c, u_1r) = 1$ as well as $e^{\frac{2\pi i(b+t(u_1p))}{(u_1p)r}}$ and $e^{\frac{2\pi i(c+s(u_1r))}{(u_1r)p}}$ are the corresponding roots of $f_{u_1,p}(q^r)$ and $f_{u_1,r}(q^p)$ for $0 \leqslant t \leqslant r-1$ and $0 \leqslant s \leqslant p-1$. Note that $b + t(u_1p)$ is congruent to b modulo u_1 and $c + s(u_1r)$ is congruent to c modulo u_1. Let $\alpha = e^{\frac{2\pi iw}{u_1p}}$ be a root of $P_{u_1,p}(q)$ which is not a root of $f_{u_1,p}(q)$. As before, w is represented by the tuple $(w_p, (w_{p_j})_j)$ where $w_p \in \{0, \ldots, p-1\}$ and $w_{p_j} \in (\mathbb{Z}/(p_j)^{h_j}\mathbb{Z})^*$ for each prime p_j dividing u_1 and h_j the highest power of p_j dividing u_1. Therefore all the elements of $\mathcal{R}_\alpha := \{e^{\frac{2\pi i(w+t(u_1p))}{(u_1p)r}} \mid t = 0, \ldots, r-1\}$ are not roots of $f_{u_1,p}(q^r)$. Note that every element of $\mathcal{R}_\alpha$ is a primitive u_1pr-root of unity since r divides u_1. Let $\beta = e^{\frac{2\pi iv}{u_1p}}$ be any root of $f_{u_1,p}(q)$ such that $v \equiv w \pmod{u_1}$. Then v is distinct from w modulo p. Then all elements of $\mathcal{R}_\beta := \{e^{\frac{2\pi i(v+t(u_1p))}{(u_1p)r}} \mid t = 0, \ldots, r-1\}$ are roots of $f_{u_1,p}(q^r)$. Note also that every element of $\mathcal{R}_\beta$ is a primitive u_1pr-root of unity since r divides u_1. Therefore, every element of $\mathcal{R}_\beta$ is a root of $f_{u,r}(q^p)$. This means that there exists a root $\gamma = e^{\frac{2\pi ic'}{u_1r}}$ of $f_{u_1,r}(q)$ where $1 \leqslant c' \leqslant u_1r - 1$ and $(c', u_1r) = 1$ such that the collection $\mathcal{R}_\gamma := \{e^{\frac{2\pi i(c'+s(u_1r))}{(u_1r)p}} \mid s = 0, \ldots, p-1,\ (c' + s(u_1r), u_1rp) = 1\}$ of root of $f_{u_1,r}(q^p)$ intersects $\mathcal{R}_\beta$. Therefore, $c' \equiv v \equiv w \pmod{u_1}$. Since p does not divide u_1r, there exists an integer $s' \in \{0, \ldots, p-1\}$ such that $c' + s'(u_1r) \equiv w \pmod{p}$, and hence $c' + s'(u_1r)$ is nonzero modulo p. Therefore $e^{\frac{2\pi i(c'+s'(u_1r))}{(u_1r)p}}$ is a primitive u_1pr-root of unity and thus must be a root of $f_{u_1,p}(q^r)$ by Functional Equation (1). In other word, $e^{\frac{2\pi i(c'+s'(u_1r))}{(u_1r)p}}$ is contained in $\mathcal{R}_\delta$ for some root δ of $f_{u_1,p}(q)$ different from α. Moreover, $c' + s'(u_1r) \equiv w \pmod{p}$ implies that $c' + s'(u_1r) \neq v \pmod{p}$. If $\delta = e^{\frac{2\pi ig}{u_1p}}$ is any root of $f_{u_1,p}(q)$ different from α, then either $g \neq w \pmod{u_1}$ or $g \neq w \pmod{p}$. As a result, either $c' \neq g \pmod{u_1}$ or $c' + s'(u_1r) \neq g \pmod{p}$. Therefore $e^{\frac{2\pi i(c'+s'(u_1r))}{(u_1r)p}}$ cannot be contained in any $\mathcal{R}_\delta$ for any $\delta \neq \alpha$. This is a contradiction. Therefore for each primitive residue class d modulo u_1, if one element in the collection of primitive u_1p-roots of unity represented by $\{(d, e) \mid 1 \leqslant e \leqslant p-1\}$ is a root of $f_{u_1,p}(q)$, then all elements in this collection are also.

Since r divides u_1, it can be verified that the collection of all roots of $f_{u_1,r}(q)$ corresponds, via CRT, to the collection of tuples $\{(w_r + t(r^l), (w_{p_j})_{j,p_j\neq r}) \mid 0 \leqslant t \leqslant r-1,\ w_r \in (\mathbb{Z}/r^l\mathbb{Z})^*,\ w_{p_j} \in (\mathbb{Z}/p_j^{h_j}\mathbb{Z})^*\}$ where $r^l \| u_1$. Let us show the other direction (see Definition 3.19), i.e. to show that if one element

of the collection $\{(w_r + t(r^l), (w_{p_j})_{j,p_j\neq r}) \mid 0 \leqslant t \leqslant r-1\}$ is a root of $f_{u_1,r}(q)$, then so are all the elements in this collection. Suppose $\alpha = e^{\frac{2\pi ic}{u_1 r}}$ is root of $P_{u_1,r}(q)$ which is not a root of $f_{u_1,r}(q)$. Then all the elements of $\mathcal{R}_\alpha := \{e^{\frac{2\pi i(c+t(u_1 r))}{(u_1 r)p}} \mid t = 0,\dots,p-1,\ (c+t(u_1 r), u_1 rp) = 1\}$ are not roots of $f_{u_1,r}(q^p)$. By construction, every element of $\mathcal{R}_\alpha$ is a primitive $u_1 pr$-root of unity. Let c, and thus α, be represented by the tuple $(c_r + z(r^l), (c_j)_{j,p_j\neq r})$ for some integer z in $\{0,\dots,r-1\}$ where $c_r \in (\mathbb{Z}/r^l\mathbb{Z})^*$ and $c_j \in (\mathbb{Z}/p_j^{h_j}\mathbb{Z})^*$. Suppose that $\beta = e^{\frac{2\pi id}{u_1 r}}$ is a root of $f_{u_1,r}(q)$ such that $d \equiv c_j \pmod{p_j^{h_j}}$ for all $p_j \neq r$, $d \equiv c_r \pmod{r^l}$ but $d \neq c \pmod{r^{l+1}}$ where c_r and c_j's are as in the representation of c above. Thus d is represented by the tuple $(c_r + z'(r^l), (c_j)_{j,p_j\neq r})$ for some integer z', different from z, in $\{0,\dots,r-1\}$. Then all the elements of the collection $\mathcal{R}_\beta := \{e^{\frac{2\pi i(d+t(u_1 r))}{(u_1 r)p}} \mid t = 0,\dots,p-1,\ (d+t(u_1 r), u_1 rp) = 1\}$ are primitive $u_1 pr$-roots of unity which are roots of $f_{u_1,r}(q^p)$ and thus must be root of $f_{u_1,p}(q^r)$ by Functional Equation (1). Thus there exists a root $\gamma = e^{\frac{2\pi ib}{u_1 p}}$ of $f_{u_1,p}(q)$ where $1 \leqslant b \leqslant u_1 p-1$ and $(b, u_1 p) = 1$ such that the collection $\mathcal{R}_\gamma := \{e^{\frac{2\pi i(b+s(u_1 p))}{(u_1 p)r}} \mid s = 0,\dots,r-1\}$ of root of $f_{u_1,p}(q^r)$, all of which are primitive $u_1 pr$-roots of unity since r divides u_1, intersects $\mathcal{R}_\beta$. Hence there exist $t' \in \{0,\dots,p-1\}$ and $s' \in \{0,\dots,r-1\}$ such that $d + t'(u_1 r) = b + s'(u_1 p)$. Thus $d \equiv b \pmod{u_1}$ which means that $d \equiv b \pmod{r^l}$ and $d \equiv b \pmod{p_j^{h_j}}$ for all p_j, different from r, dividing u_1. Thus $c \equiv b \pmod{r^l}$ and $c \equiv b \pmod{p_j^{h_j}}$ for all p_j, different from r, dividing u_1. Since sp are distinct modulo r for $0 \leqslant s \leqslant r-1$, there exists $s'' \in \{0,\dots,r-1\}$ such that $b + s''(u_1 p) \equiv c_r + z(r^l) \equiv c \pmod{r^{l+1}}$. Therefore, $e^{\frac{2\pi i(b+s''(u_1 p))}{(u_1 p)r}}$ is a primitive $u_1 pr$-root of unity and thus must be a root of $f_{u_1,r}(q^p)$ by Functional Equation (1). Thus $e^{\frac{2\pi i(b+s''(u_1 p))}{(u_1 p)r}}$ must be contained in $\mathcal{R}_\delta$ for some root δ of $f_{u_1,r}(q)$ different from α. Let $\delta = e^{\frac{2\pi iy}{u_1 r}}$ be any root of $f_{u_1,r}(q)$ different from α with $1 \leqslant y \leqslant u_1 r-1$, then $\mathcal{R}_\delta := \{e^{\frac{2\pi i(y+t(u_1 r))}{(u_1 r)p}} \mid t = 0,\dots,p-1,\ (y+t(u_1 r), u_1 rp) = 1\}$. Then either $y \neq c \pmod{p_j}$ for at least one p_j dividing u_1 different from r or $y \neq c \pmod{r^{l+1}}$. Hence $b + s''(u_1 p) \neq y + t(u_1 r) \pmod{u_1 pr}$ for any $t \in \{0,\dots,p-1\}$ such that $(y+t(u_1 r), u_1 rp) = 1$. Therefore, $e^{\frac{2\pi i(b+s(u_1 p))}{(u_1 p)r}}$ cannot be contained in $\mathcal{R}_\delta$ for any root δ of $f_{u_1,r}(q)$ different from α. This is again a contradiction. Therefore, if one element of the collection $\{(w_r + t(r^l), (w_{p_j})_{j,p_j\neq r}) \mid 0 \leqslant t \leqslant r-1\}$ is a root of $f_{u_1,r}(q)$, then so are all the elements in this collection as required.

(b) pr divides u_1: Again the collection of roots of $f_{u_1,p}(q)$ corresponds via CRT to the collection of tuples $\{(w_p + t(p^h), (w_{p_j})_{j,p_j\neq p}) \mid w_p \in (\mathbb{Z}//p^h\mathbb{Z})^*,\ w_{p_j} \in (\mathbb{Z}//p_j^{h_j}\mathbb{Z})^*\}$ where $t = 0,\dots,p-1$, $p^h \| u_1$, $r := p_0$ and $l := h_0$ where $r^l \| u_1$. We need to show that if one element of the collection $\{(w_p + t(p^h), (w_{p_j})_{j,p_j\neq p}) \mid 0 \leqslant t \leqslant p-1\}$ corresponds to a root of $f_{u_1,p}(q)$, then so does all elements of this collection. Suppose that $\alpha = e^{\frac{2\pi ia}{u_1 p}}$ is a root of $P_{u_1,p}(q)$ which is not a root of $f_{u_1,p}$ where $1 \leqslant a \leqslant u_1 p-1$. Then none of the elements of the collection $\mathcal{R}_\alpha = \{e^{\frac{2\pi i(a+s(u_1 p))}{(u_1 p)p_0}} \mid s = 0,\dots,p_0-1\}$ is a root of $f_{u_1,p}(q^{p_0})$. Let a, and thus α, be represented by the tuple $(a_p + z(p^h), (a_j)_{j,p_j\neq p})$ for some integer z in $\{0,\dots,p-1\}$ where $a_p \in (\mathbb{Z}/p^h\mathbb{Z})^*$ and $a_j \in (\mathbb{Z}/p_j^{h_j}\mathbb{Z})^*$. Suppose $\beta = e^{\frac{2\pi ib}{u_1 p}}$ is a root of $f_{u_1,p}(q)$ where $1 \leqslant b \leqslant u_1 p-1$ such that $b \equiv a \pmod{p_j^{h_j}}$ for each p_j dividing u_1 different from p and $b \equiv a \pmod{p^h}$ but $b \neq a \pmod{p^{h+1}}$. Then every element in the collection $\mathcal{R}_\beta = \{e^{\frac{2\pi i(b+t(u_1 p))}{(u_1 p)p_0}} \mid t = 0,\dots,p_0-1\}$ is a root of $f_{u_1,p}(q^{p_0})$ as well as a primitive $u_1 pp_0$-root of unity since p_0 divides u_1. Therefore, every element of $\mathcal{R}_\beta$ is a root of $f_{u_1,p_0}(q^p)$ by Functional Equation (1). This implies that there is a root $\gamma = e^{\frac{2\pi ig}{u_1 p_0}}$ of $f_{u_1,p_0}(q)$ where $0 \leqslant g \leqslant u_1 p_0 - 1$ such that $\mathcal{R}_\gamma = \{e^{\frac{2\pi i(g+x(u_1 p_0))}{(u_1 p_0)p}} \mid x = 0,\dots,p-1\}$ intersects $\mathcal{R}_\beta$. Thus $g \equiv b \pmod{p_j^{h_j}}$ for all p_j dividing u_1 different from p. Note that all the elements of $\{xp_0 \mid x = 0,\dots,p-1\}$ are distinct modulo p. Therefore,

there exists $x' \in \{x = 0, \ldots, p-1\}$ such that $g + x''(u_1 p_0) \equiv b \pmod{p^{h+1}}$. Thus $e^{\frac{2\pi i(g+x''(p^h))}{(u_1 r)p}}$ must belong to $\mathcal{R}_\delta$, the collection of all r-roots of δ, for some root δ of $f_{u_1,p}(q)$ different from α. By a similar argument as before, this leads to a contradiction. By symmetry, the opposite direction follows, i.e. if one element of the collection of tuples $\{(w_r + t(r^l), (w_{p_j})_{j,p_j \neq r}) \mid w_r \in (\mathbb{Z}//r^l\mathbb{Z})^*,\ w_{p_j} \in (\mathbb{Z}//p_j^{h_j}\mathbb{Z})^*\}$ where $t = 0, \ldots, r-1$, $r^l \| u_1$, $p := p_0$ and $h := h_0$ corresponds to a root of $f_{u_1,r}(q)$, then so does all the elements of this collection.

Let $\square$ denote either p or r and α be a root of $f_{u_1,\square}(q)$. Then it is of the form $e^{\frac{2\pi i w}{u_1 \square}}$ for some $1 \leqslant w \leqslant u_1\square - 1$ which is relatively prime to $u_1\square$. We denote such a root by w. Let $u_1 = \prod_j p_j^{g_j}$ be the prime factorization of u_1. Let $((d_j)_j, w_\square)$ where $d_j \in (\mathbb{Z}/p_j^{g_j}\mathbb{Z})^*$ and $1 \leqslant w_\square \leqslant \square - 1$ be the tuple corresponding to w by the Chinese Remainder Theorem. We also refer to w (and thus the root represented by w) by this tuple. Let $\{1^*_\square, \ldots, \square - 1\}$ be defined as follows: $1^*_\square = 0$ if $\square$ divides u_1 and $1^*_\square = 1$ otherwise. Also, let $1^*_{pr} := (1^*_p, 1^*_r)$ and vice versa for 1^*_{rp}. This allows us to prove (3) simultaneously for all four cases: pr does not divide u_1; either p or r divides u_1 but not both; and pr divides u_1.

It is straightforward to verify, using Key Proposition 1 (the details of which are left to the readers), that (3) follows from the following statements:

(i) For each $a \in \{1^*_p, \ldots, p-1\}$ and $b \in \{1^*_r, \ldots, r-1\}$, the set of unordered tuples $\{(d_j)_j \mid d_j \in (\mathbb{Z}/p_j^{g_j}\mathbb{Z})^*\}$ with multiplicity such that if $1^*_p = 1$ (resp. $1^*_p = 0$), $((d_j)_j, a)$ (resp. $((d_j)_{j,p_j\neq p}, d_{(p)} + ap^h)$ where h is the highest power of p dividing u_1 and $d_{(p)} = d_k$ where $p_k = p$) is a root of $f_{u_1,p}(q)$ is the same as the set of unordered tuples $\{(e_j)_j \mid e_j \in (\mathbb{Z}/p_j^{g_j}\mathbb{Z})^*\}$ such that if $1^*_r = 1$ (resp. $1^*_r = 0$), $((e_j)_j, b)$ (resp. $((e_j)_{j,p_j\neq r}, e_{(r)} + br^l)$) is a root of $f_{u_1,r}(q)$ where l is the highest power of r dividing u_1 and $e_{(r)} = e_s$ where $p_s = r$.

(ii) If $1^*_\square = 1$ (resp. $1^*_\square = 0$), then any unordered tuple of integers in the set $\{((d_j)_j, a) \mid 1 \leqslant a \leqslant \square - 1,\ d_j \in (\mathbb{Z}/p_j^{g_j}\mathbb{Z})^*\}$ (resp. $((d_j)_{j,p_j\neq\square}, d_{(\square)} + a\square^{h_\square})$ where $h_\square$ is the highest power of $\square$ dividing u_1, $d_{(\square)} = d_k$ where $p_k = \square$ and $0 \leqslant a \leqslant \square - 1$) is a root of $f_{u_1,\square}(q)$ if an only if every unordered tuple in this set must also be a root of $f_{u_1,\square}(q)$.

We prove these by comparing the number of primitive roots of unity of order $u_1 pr$ which are roots of $f_{u_1,p}(q) f_{u_1,r}(q^p)$ and $f_{u_1,r}(q) f_{u_1,p}(q^r)$ (or more specifically, roots of $f_{u_1,r}(q^p)$ and of $f_{u_1,p}(q^r)$). In the proof below, if p (resp. r) divides u_1, we denote by h (resp. l) the highest power of p (resp. r) dividing u_1.

(i) From the proof of (1) above, $f_{u_1,\square}(q)$ is nontrivial where $\square$ denotes either p or r. Thus there exists $a_0 \in \{1^*_p, \ldots, p-1\}$ such that $((d_j)_j, a_0)$ if $1^*_p = 1$ (resp. $((d_j)_{j,p_j\neq p}, d_{(p)} + a_0 p^h)$ if $1^*_p = 0$) is a root of $f_{u_1,p}(q)$ for some unordered tuples $(d_j)_j$ of integers with $d_j \in (\mathbb{Z}/p_j^{g_j}\mathbb{Z})^*$ and $d_{(p)} = d_k$ where $p_k = p$. Let $(\hat{d}_j)_j$ be one such tuple and $z_{a_0,p}$ be its multiplicity, i.e. the highest power of $(q - \alpha)$ dividing $f_{u_1,p}(q)$ where α is represented by $((\hat{d}_j)_j, a_0)$ if $1^*_p = 1$ (resp. $((\hat{d}_j)_{j,p_j\neq p}, \hat{d}_{(p)} + a_0 p^h)$ if $1^*_p = 0$). For each $b \in \{1^*_r, \ldots, r-1\}$, the set of rth-roots of $((\hat{d}_j)_j, a_0)$ if $1^*_p = 1$ (resp. $((\hat{d}_j)_{j,p_j\neq p}, \hat{d}_{(p)} + a_0 p^h)$ if $1^*_p = 0$) which are primitive $u_1 pr$-roots of unity must all be roots of $f_{u_1,p}(q^r)$. Let $\mathcal{A}_b$ be the set consisting of all roots of $f_{u_1,p}(q^r)$, with multiplicity, of the form $\{((\hat{d}_j)_j, b, a_0)\}$ if $1^*_{pr} = (1,1)$ and $\{((\hat{d}_j)_{j,p_j\neq r}, d_{(r)} + br^l, a_0)\}$ if $1^*_{pr} = (1,0)$ (resp. $\{((\hat{d}_j)_{j,p_j\neq p}, b, \hat{d}_{(p)} + a_0 p^h)\}$ if $1^*_{pr} = (0,1)$ and $\{((\hat{d}_j)_{j,p_j\neq p,r}, \hat{d}_{(r)} + br^l, \hat{d}_{(p)} + a_0 p^h)\}$ if $1^*_{pr} = (0,0)$). Then it has cardinality $z_{a_0,p}$ for each b. Therefore these are also all the roots of $f_{u_1,r}(q^p)$ which are primitive $u_1 pr$-roots of unity of the form listed above for each $b \in \{1^*_r, \ldots, r-1\}$. Now let $b_0 \in \{1^*_r, \ldots, r-1\}$. Let $z_{b_0,r}$ be the highest power of $(q-\beta)$ dividing $f_{u_1,r}(q)$ where β is represented by $((\hat{d}_j)_j, b_0)$ if $1^*_r = 1$ (resp. $\{((\hat{d}_j)_{j,p_j\neq r}, \hat{d}_{(r)} + b_0 r^l)\}$ if $1^*_r = 0$) where $\hat{d}_{(r)} = p_s$ and $p_s = r$. For each $a \in \{1^*, \ldots, p-1\}$, the set of pth-roots of $((\hat{d}_j)_j, b_0)$ if $1^*_r = 1$ (resp. $((\hat{d}_j)_{j,p_j\neq r}, \hat{d}_{(r)} + b_0 r^h)$ if $1^*_r = 0$) which are primitive $u_1 pr$-roots of unity must all be roots of $f_{u_1,r}(q^p)$. Let $\mathcal{B}_a$ be the set consisting of all roots of $f_{u_1,r}(q^p)$, with multiplicity, of the form $\{((\hat{d}_j)_j, a, b_0)\}$ if $1^*_{rp} = (1,1)$ and $\{((\hat{d}_j)_{j,p_j\neq p}, d_{(p)} + ap^h, b_0)\}$ if $1^*_{rp} = (1,0)$ (resp. $\{((\hat{d}_j)_{j,p_j\neq p}, a, \hat{d}_{(r)} +$

$b_0 r^l)\}$ if $1^*_{rp} = (0,1)$ and $\{((\hat{d}_j)_{j,p_j\neq p,r}, \hat{d}_{(p)} + ap^h, \hat{d}_{(r)} + b_0 r^l)\}$ if $1^*_{rp} = (0,0)$). Then it has cardinality $z_{b_0,r}$ for each a. These are all the roots of $f_{u_1,r}(q^p)$ (and thus of $f_{u_1,p}(q^r)$ by Functional Equation (1)) which are primitive $u_1 pr$-roots of unity of the forms just listed. Then the cardinality of $\mathcal{A}_{b_0}$ is equal to the cardinality of $\mathcal{B}_{a_0}$. Therefore $z_{a_0,p} = z_{b_0,r}$ and (i) is proved. We denote this common value by z.

(ii) Let $(d_j)_j$ be a tuple of integers where $d_j \in (\mathbb{Z}/p_j^{g_j}\mathbb{Z})^*$ for each j such that there exists an $a_0 \in \{1^*_p, \dots, p-1\}$ with $((d_j)_j, a_0)$ (resp. $((d_j)_{j,p_j\neq p}, d_{(p)} + a_0 p^h)$) being a root of $f_{u_1,p}(q)$ if $1^*_p = 1$ (resp. if $1^*_p = 0$). As a result, the set of roots of $f_{u_1,p}(q^r)$ which are primitive $u_1 pr$-roots of unity, contains those of the form $\{((d_j)_j, b, a_0)\}$ if $1^*_{pr} = (1,1)$ or $\{((d_j)_{j,p_j\neq r}, d_{(r)} + br^l, a_0)\}$ if $1^*_{pr} = (1,0)$ (resp. $\{((d_j)_{j,p_j\neq p}, b, d_{(p)} + a_0 p^h)\}$ if $1^*_{pr} = (0,1)$ or $\{((d_j)_{j,p_j\neq p,r}, d_{(r)} + br^l, d_{(p)} + a_0 p^h)\}$ if $1^*_{pr} = (0,0)$) for each $b \in \{1^*_r, \dots, r-1\}$. By Functional Equation (1), these are also roots of $f_{u_1,r}(q^p)$. Let b_0 be any element of the set $\{1^*_r, \dots, r-1\}$. Then by the above, $((d_j)_j, b_0, a_0)$ if $1^*_{pr} = (1,1)$ or $((d_j)_{j,p_j\neq r}, d_{(r)} + b_0 r^l, a_0)$ if $1^*_{pr} = (1,0)$ (resp. $\{((d_j)_{j,p_j\neq p}, b_0, d_{(p)} + a_0 p^h)\}$ if $1^*_{pr} = (0,1)$ or $\{((d_j)_{j,p_j\neq p,r}, d_{(r)} + b_0 r^l, d_{(p)} + a_0 p^h)\}$ if $1^*_{pr} = (0,0)$) corresponds to a primitive $u_1 pr$-root of unity which is a root of $f_{u_1,p}(q^r)$ and thus of $f_{u_1,r}(q^p)$ by Functional Equation (1). Therefore $((d_j)_j, b_0)$ (resp. $((d_j)_{j,p_j\neq r}, d_{(r)} + b_0 r^l)$) if $1^*_r = 1$ (resp. $1^*_r = 0$) must be a root of $f_{u_1,r}(q)$, which in turn means that every element of the set $\{((d_j)_j, b_0, a)\}$ if $1^*_{pr} = (1,1)$ or $\{((d_j)_{j,p_j\neq r}, d_{(r)} + b_0 r^l, a)\}$ if $1^*_{pr} = (1,0)$ (resp. $\{((d_j)_{j,p_j\neq p}, b_0, d_{(p)} + ap^h)\}$ if $1^*_{pr} = (0,1)$ or $\{((d_j)_{j,p_j\neq p,r}, d_{(r)} + b_0 r^l, d_{(p)} + ap^h)\}$ if $1^*_{pr} = (0,0)$) for $1^*_p \leqslant a \leqslant p-1$ must also be roots of $f_{u_1,r}(q^p)$ and thus of $f_{u_1,p}(q^r)$. This means that every element of the set $\{((d_j)_j, a) \mid 1 \leqslant a \leqslant p-1\}$ if $1^* = 1$ (resp. $\{((d_j)_{j,p_j\neq p}, d_{(p)} + ap^h) \mid 0 \leqslant a \leqslant p-1\}$ if $1^* = 0$) must be a root of $f_{u_1,p}(q)$. By a similar argument, if $((d_j)_j, b_0)$ for $1^*_r = 1$ (resp. $((d_j)_{j,p_j\neq r}, d_{(r)} + b_0 r^l)$ for $1^*_r = 0$) is a root of $f_{u_1,r}(q)$, then every element of the set $\{((d_j)_j, b_0) \mid 1 \leqslant b \leqslant r-1\}$ (resp. $\{((d_j)_{j,p_j\neq r}, d_{(r)} + b_0 r^l) \mid 0 \leqslant b \leqslant r-1\}$) is also a root of $f_{u_1,r}(q)$. Thus (ii) is proved. Since (3) is equivalent to (i) and (ii), the result follows.

(4) Let p and r be two distinct primes in the support of Γ. For proving (4), we may assume without loss of generality that pr does not divide $v_{p,r,k}$ for any k. Consider EFE(1) with respect to p and r:

$$\begin{array}{ccc}
f_{v_{p,r,1},p}(q)^{s_{p,1}} f_{v_{p,r,1},r}\big(q^p\big)^{s_{r,1}} & \overset{(1)}{\longleftrightarrow} & f_{v_{p,r,1},r}(q)^{s_{r,1}} f_{v_{p,r,1},p}\big(q^r\big)^{s_{p,1}} \\
\cdots & \cdots & \cdots \\
f_{v_{p,r,k},p}(q)^{s_{p,k}} f_{v_{p,r,k},r}\big(q^p\big)^{s_{r,k}} & \overset{(k)}{\longleftrightarrow} & f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}} f_{v_{p,r,k},p}\big(q^r\big)^{s_{p,k}} \\
\cdots & \cdots & \cdots \\
f_p(q) f_r\big(q^p\big) & = & f_r(q) f_p\big(q^r\big).
\end{array}$$

Let us select an arbitrary line of EFE(1) above, say (k). Then there are two possibilities:

(a) r divides $v_{p,r,k}$ and p does not or vice versa: In this case, we may suppose without loss of generality that r divides $v_{p,r,k}$ and p does not as well as $s_{r,k} = 1$. Then line (k) of the reduced form must be

$$f_{v_{p,r,k},p}(q) \frac{f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q)} \overset{(k)}{\longleftrightarrow} f_{v_{p,r,k},p}\big(q^r\big).$$

We claim that the rational function on the left-hand side above must be a polynomial. Let us suppose otherwise. From our analysis of $f_{v_{p,r,k},r}(q^p)$ earlier, we know that there exists a polynomial $f'_{v_{p,r,k},r}(q) \in \mathbb{C}[q]$ satisfying the following conditions:

(i) $\deg(f'_{v_{p,r,k},r}(q)) = \deg(f_{v_{p,r,k},r}(q))$.
(ii) $f'_{v_{p,r,k},r}(q)$ divides $f_{v_{p,r,k},r}(q^p)$ in $\mathbb{C}[q]$.

(iii) Every root of $f'_{v_{p,r,k},r}(q)$ is a primitive $v_{p,r,k}r$-root of unity.

(iv) Every root of $\frac{f_{v_{p,r,k},r}(q^p)}{f'_{v_{p,r,k},r}(q)}$ is a primitive $v_{p,r,k}pr$-root of unity.

As a result of our assumption above, there must exist at least one root of $f'_{v_{p,r,k},r}(q)$, say α, which is not a root of $(f_{v_{p,r,k},r}(q))$. From EFE(1) above, this means that there exists a level $l \neq k$ such that α is a root of the polynomial $f_{v_{p,r,l},r}(q)^{s_{r,l}} f_{v_{p,r,l},p}(q^r)^{s_{p,l}}$. Since $v_{p,r,l} \neq v_{p,r,k}$, α must be a root of $f_{v_{p,r,l},p}(q^r)^{s_{p,l}}$ and thus $s_{p,l} = 1$. However, every root of $f_{v_{p,r,l},p}(q^r)$ is either a primitive $v_{p,r,l}p$-root of unity or a primitive $v_{p,r,l}pr$-root of unity by our prior analysis. Therefore either $v_{p,r,k}r = v_{p,r,l}p$ or $v_{p,r,k}r = v_{p,r,l}pr$. This means that either $v_{p,r,k} = \frac{v_{p,r,l}p}{r}$ or $v_{p,r,k} = v_{p,r,l}p$. In either cases, p must divide $v_{p,r,k}$. This contradicts our assumption. Thus the result follows.

(b) Both p and r do not divide $v_{p,r,k}$: We may suppose that $s_{p,k} = s_{r,k} = 1$ since otherwise there is nothing to prove. Then line (k) of the reduced form of EFE(1) with respect to p and r has the form

$$\frac{f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q)} \overset{(k)}{\longleftrightarrow} \frac{f_{v_{p,r,k},p}(q^r)}{f_{v_{p,r,k},p}(q)}.$$

Suppose that $\frac{f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q)}$ is not a polynomial. Then an exact argument as in part (a) produces a contradiction. Suppose that $\frac{f_{v_{p,r,k},p}(q^r)}{f_{v_{p,r,k},p}(q)}$ is not a polynomial. Then an argument similar to part (a) above with p replaced by r also produces a contradiction. Therefore $\frac{f_{u_1,p}(q^r)}{f_{u_1,p}(q)}$ and $\frac{f_{u_1,r}(q^p)}{f_{u_1,r}(q)}$ are polynomials whenever they occur in the reduced form of EFE(1) with respect to p and r. Thus (4) is proved.

(ii) Without loss of generality, we may assume $\square = p$ and $\triangle = r$. Let $P_{u,p}(q)$ denote the cyclotomic polynomial with coefficients in $\mathbb{Q}$ of order up. Let m_p be the highest power of $P_{u,p}(q)$ dividing $f_{u,p}(q)$ and n_p be the lowest power of $P_{u,p}(q)$ such that $f_{u,p}(q)$ divides $(P_{u,p}(q))^{n_p}$. Then

$$\frac{f_{u,p}(q)}{(P_{u,p}(q))^{m_p}} \neq 1$$

since $f_{u,p}(q)$ is not a polynomial in $\mathbb{Q}[q]$ by hypothesis. It can be verified that $P_{u,p}(q)$ does not divide $\frac{f_{u,p}(q)}{(P_{u,p}(q))^{m_p}}$ and $\frac{f_{u,p}(q)}{(P_{u,p}(q))^{m_p}}$ divides $(P_{u,p}(q))^{n_p - m_p}$. Let $\pi_{u,p}(q) := (\frac{f_{u,p}(q)}{(P_{u,p}(q))^{m_p}}, P_{u,p}(q))$, the greatest common factor of $\frac{f_{u,p}(q)}{(P_{u,p}(q))^{m_p}}$ and $P_{u,p}(q)$. Then $\pi_{u,p}(q)$ is a nontrivial polynomial with coefficients not contained in $\mathbb{Q}$ which properly divides $P_{u,p}(q)$. Moreover, it can be verified that if α is a root of $f_{u,p}(q)$, then α is also a root of $\pi_{u,p}(q)$. Let us denote $\pi_{u,p}(q)$ by $\pi^{(0)}_{u,p}(q)$. Let e_0 be the greatest positive integer such that $(\pi^{(0)}_{u,p}(q))^{e_0}$ divides $f_{u,p}(q)$. Let $\pi^{(i)}_{u,p}(q)$ be defined as follows.

$$\pi^{(i)}_{u,p}(q) = \begin{cases} (\frac{f_{u,p}(q)}{\prod_{0 \leqslant j < i} (\pi^{(j)}_{u,p}(q))^{e_j}}, P_{u,p}(q)) & \text{if } (\frac{f_{u,p}(q)}{\prod_{0 \leqslant j < i} (\pi^{(j)}_{u,p}(q))^{e_j}}, P_{u,p}(q)) \neq 1, \\ 1 & \text{otherwise,} \end{cases}$$

where:

- $(\cdot,\cdot)$ denotes the greatest common divisor symbol.
- e_j denotes the greatest positive integer such that $(\pi^{(j)}_{u,p}(q))^{e_j}$ divides

$$\frac{f_{u,p}(q)}{\prod_{0 \leqslant s < j-1} (\pi^{(s)}_{u,p}(q))^{e_s}}.$$

It can be verified that there exists a nonnegative integer z such that $\pi_{u,p}^{(z)}(q) \neq 1$ and $\pi_{u,p}^{(j)}(q) = 1$ for all $j > z$. As a result,

$$f_{u,p}(q) = \prod_{0 \leqslant j \leqslant z} (\pi_{u,p}^{(j)}(q))^{e_j}$$

and thus

$$\frac{f_{u,p}(q^r)}{f_{u,p}(q)} = \prod_{0 \leqslant j \leqslant z} \frac{(\pi_{u,p}^{(j)}(q^r))^{e_j}}{\pi_{u,p}^{(j)}(q)^{e_j}}.$$

Lemma 3.21.

$$\frac{f_{u,p}(q^r)}{f_{u,p}(q)}$$

is a polynomial if and only if

$$\frac{\pi_{u,p}^{(j)}(q^r)}{\pi_{u,p}^{(j)}(q)}$$

is a polynomial for all $j \in \{0, \ldots, z\}$.

Proof. One direction is obvious. Suppose that $\frac{f_{u,p}(q^r)}{f_{u,p}(q)}$ is a polynomial. It can be deduced from the proof of Key Proposition 1 that r does not divide u since otherwise $f_{u,p}(q^r)$ would be a nontrivial monic polynomial whose roots are primitive upr-roots of unity while $f_{u,p}(q)$ is a nontrivial monic polynomial whose roots are primitive up-roots of unity. We can rewrite $\frac{f_{u,p}(q^r)}{f_{u,p}(q)}$ as

$$\frac{f_{u,p}(q^r)}{f_{u,p}(q)} = \frac{P_{u,p}(q^r)^{m_p} \frac{f_{u,p}(q^r)}{P_{u,p}(q^r)^{m_p}}}{P_{u,p}(q)^{m_p} \frac{f_{u,p}(q)}{P_{u,p}(q)^{m_p}}} = \frac{P_{u,p}(q^r)^{m_p}}{P_{u,p}(q)^{m_p}} \frac{\frac{f_{u,p}(q^r)}{P_{u,p}(q^r)^{m_p}}}{\frac{f_{u,p}(q)}{P_{u,p}(q)^{m_p}}}.$$

It can be verified that $\frac{P_{u,p}(q^r)}{P_{u,p}(q)}$ is a monic polynomial whose roots are primitive upr-roots of unity. On the other hand, $\frac{f_{u,p}(q)}{P_{u,p}(q)^{m_p}}$ is a monic polynomial whose roots are primitive up-roots of unity. Hence,

$$\left(\frac{P_{u,p}(q^r)}{P_{u,p}(q)}, \frac{f_{u,p}(q)}{P_{u,p}(q)^{m_p}}\right) = 1$$

where (u, v) denotes the greatest common factor of u and v. Therefore,

$$\frac{\frac{f_{u,p}(q^r)}{P_{u,p}(q^r)^{m_p}}}{\frac{f_{u,p}(q)}{P_{u,p}(q)^{m_p}}}$$

must also be a polynomial. As a result, we may assume without loss of generality that $m_p = 0$. Let us denote $\pi_{u,p}(q)$ by $\pi_{u,p}^{(0)}(q)$. Let e_0 be the greatest positive integer such that $(\pi_{u,p}^{(0)}(q))^{e_0}$ divides $f_{u,p}(q)$. Let $\pi_{u,p}^{(i)}(q)$ be defined as follows.

$$\pi_{u,p}^{(i)}(q) = \begin{cases} \left(\frac{f_{u,p}(q)}{\prod_{0\leqslant j<i}(\pi_{u,p}^{(j)}(q))^{e_j}}, P_{u,p}(q)\right) & \text{if } \left(\frac{f_{u,p}(q)}{\prod_{0\leqslant j<i}(\pi_{u,p}^{(j)}(q))^{e_j}}, P_{u,p}(q)\right) \neq 1, \\ 1 & \text{otherwise.} \end{cases}$$

where:

- $(\cdot,\cdot)$ denotes the greatest common divisor symbol.
- e_j denotes the greatest positive integer such that $(\pi_{u,p}^{(j)}(q))^{e_j}$ divides

$$\frac{f_{u,p}(q)}{\prod_{0\leqslant s<j-1}(\pi_{u,p}^{(s)}(q))^{e_s}}.$$

It can be verified that there exists a nonnegative integer z such that $\pi_{u,p}^{(z)}(q) \neq 1$ and $\pi_{u,p}^{(j)}(q) = 1$ for all $j > z$. As a result,

$$f_{u,p}(q) = \prod_{0\leqslant j\leqslant z} \left(\pi_{u,p}^{(j)}(q)\right)^{e_j}$$

and thus

$$\frac{f_{u,p}(q^r)}{f_{u,p}(q)} = \prod_{0\leqslant j\leqslant z} \frac{(\pi_{u,p}^{(j)}(q^r))^{e_j}}{\pi_{u,p}^{(j)}(q)^{e_j}}.$$

Furthermore, it can be verified that $\pi_{u,p}^{(j+1)}(q)$ divides $\pi_{u,p}^{(j)}(q)$ for $0 \leqslant j \leqslant z-1$. In particular, $\pi_{u,p}^{(j)}(q)$ divides $\pi_{u,p}(q)$ for $0 \leqslant j \leqslant z$. If $z = 0$, i.e. $f_{u,p}(q) = (\pi_{u,p}(q))^{e_0}$, then the lemma is trivial since

$$\frac{f_{u,p}(q^r)}{f_{u,p}(q)} = \frac{(\pi_{u,p}(q^r))^{e_0}}{\pi_{u,p}(q)^{e_0}} = \left(\frac{\pi_{u,p}(q^r)}{\pi_{u,p}(q)}\right)^{e_0}.$$

Thus we may assume that $z > 0$. Let us suppose that there exists at least one index j in $\{0,\ldots,z\}$ such that

$$\frac{\pi_{u,p}^{(j)}(q^r)}{\pi_{u,p}^{(j)}(q)}$$

is not a polynomial. Choose the smallest index j_0 among such j's. We may assume that $j_0 = 0$ since otherwise, we may replace $\frac{f_{u,p}(q^r)}{f_{u,p}(q)}$ by

$$\frac{\frac{f_{u,p}(q^r)}{\prod_{0\leqslant j\leqslant j_0}\pi_{u,p}^{(j)}(q^r)}}{\frac{f_{u,p}(q)}{\prod_{0\leqslant j\leqslant j_0}\pi_{u,p}^{(j)}(q)}}.$$

Hence, let us suppose that

$$\frac{\pi_{u,p}(q^r)}{\pi_{u,p}(q)}$$

is not a polynomial. Hence there exists at least one root, say γ, of $\pi_{u,p}(q)$ which is not a root of $\pi_{u,p}(q^r)$. Let a be the primitive residue of r modulo u. Then $a \neq 1$ and

$$\pi_{u,p}\left(q^r\right) = \pi_{ur,p}(q)\pi'_{u,p}(q)$$

by the proof of Key Proposition 1, where:

- $\pi_{ur,p}(q)$ is the factor of $\pi_{u,p}(q^r)$ whose roots are all the roots of $\pi_{u,p}(q^r)$ which are primitive upr-roots of unity.
- $\pi'_{u,p}(q)$ is the factor of $\pi_{u,p}(q^r)$ whose roots are all the roots of $\pi_{u,p}(q^r)$ which are primitive up-roots of unity such that $\pi'_{u,p}(q) \neq \pi_{u,p}(q)$ and $\deg(\pi'_{u,p}(q)) = \deg(\pi_{u,p}(q))$.

Thus γ is a primitive up-root of unity which is not a root of $\pi'_{u,p}(q)$.

By similar arguments as above,

$$\pi^{(j)}_{u,p}\left(q^r\right) = \pi^{(j)}_{ur,p}(q)\pi^{(j)\prime}_{u,p}(q)$$

for all $j \in \{0, \ldots, z\}$ where:

- $\pi^{(j)}_{ur,p}(q)$ is the factor of $\pi^{(j)}_{u,p}(q^r)$ whose roots are all the roots of $\pi^{(j)}_{u,p}(q^r)$ which are primitive upr-roots of unity.
- $\pi^{(j)\prime}_{u,p}(q)$ is the factor of $\pi^{(j)}_{u,p}(q^r)$ whose roots are all the roots of $\pi^{(j)}_{u,p}(q^r)$ which are primitive up-roots of unity such that $\pi^{(j)\prime}_{u,p}(q) \neq \pi^{(j)}_{u,p}(q)$ and $\deg(\pi^{(j)\prime}_{u,p}(q)) = \deg(\pi^{(j)}_{u,p}(q))$.

Therefore,

$$\frac{f_{u,p}(q^r)}{f_{u,p}(q)} = \prod_{0 \leqslant j \leqslant z} \frac{(\pi^{(j)}_{u,p}(q^r))^{e_j}}{\pi^{(j)}_{u,p}(q)^{e_j}} = \prod_{0 \leqslant j \leqslant z} \frac{(\pi^{(j)}_{ur,p}(q)\pi^{(j)\prime}_{u,p}(q))^{e_j}}{\pi^{(j)}_{u,p}(q)^{e_j}}.$$

Since $\pi^{(j)}_{u,p}(q)$ divides $\pi^{(j)}_{u,p}(q)$ for all $j \in \{0, \ldots, z\}$, it can be verified that

(1) $\pi^{(j)}_{ur,p}(q)$ divides $\pi_{ur,p}(q)$ for all $j \in \{0, \ldots, z\}$ and
(2) $\pi^{(j)\prime}_{u,p}(q)$ divides $\pi'_{u,p}(q)$ for all $j \in \{0, \ldots, z\}$.

Therefore, γ is not a root of $\pi^{(j)\prime}_{u,p}(q)$ for all $j \in \{0, \ldots, z\}$. Since γ is a primitive up-root of unity, γ is not a root of $\pi^{(j)}_{ur,p}(q)$ for all $j \in \{0, \ldots, z\}$. As a result, γ is not a root of $\prod_{0 \leqslant j \leqslant z}(\pi^{(j)}_{ur,p}(q)\pi^{(j)\prime}_{u,p}(q))^{e_j}$. As γ is a root of $\pi_{u,p}(q)$ and thus a root of $f_{u,p}(q)$, it follows that

$$\frac{f_{u,p}(q^r)}{f_{u,p}(q)}$$

cannot be a polynomial. This contradicts our assumption. Therefore,

$$\frac{\pi^{(j)}_{u,p}(q^r)}{\pi^{(j)}_{u,p}(q)}$$

must be a polynomial for each $j \in \{0, \ldots, z\}$. As a result, Key Proposition 1 implies that there exists a collection of sets

$$\left\{\mathcal{A}_j \;\middle|\; \mathcal{A}_{j+1} \subseteq \mathcal{A}_j;\ \mathcal{A}_j \subseteq (\mathbb{Z}/u\mathbb{Z})^*;\ j \in \{0, \ldots, z\}\right\}$$

such that:

- The collection of tuples

$$\left\{(\alpha_u, \alpha_p) \;\middle|\; \alpha_u \in \mathcal{A}_j;\ \alpha_p \in (\mathbb{Z}/p\mathbb{Z})^*\right\}$$

  represents the collection of roots of $\pi_{u,p}^{(j)}(q)$.

- $$r\mathcal{A}_j = \mathcal{A}_j$$

  for all j in $\{0, \ldots, z\}$ and

$$\mathcal{A}_j < (\mathbb{Z}/u\mathbb{Z})^*$$

  for at least one j.

It can be verified in particular that

$$r\mathcal{A}_j = \mathcal{A}_j$$

for all j in $\{0, \ldots, z\}$ if

$$r \equiv 1 \pmod{u}$$

as in Key Proposition 1. □

The proof of Key Proposition 1′ is thus complete. □

Let u be defined as in part (1) of Key Proposition 1′. Let r be any prime in $\mathcal{U}$ and p be the prime chosen in part (1) above. Hence p is strictly greater than all primes in $\mathcal{U}$; in particular, p does not divide $v_{p_i,p_j,i}$ for any $v_{p_i,p_j,i}$ appearing in EFE(1) of Γ with respect to any primes p_i and p_j.

Proposition 3.22 *(Key Proposition 2). Let $f_p(q) = \prod_j f_{u_{p,j},p}(q)$ where $f_{u_{p,j},p}(q)$ is the factor of $f_p(q)$ such that its roots are all the roots of $f_p(q)$ which are primitive $u_{p,j}p$-roots of unity for some integers $u_{p,j}$.*

(a) *Let p' be a prime different from p such that p' is not in $\mathcal{U}$. Then the reduced form of* EFE(1) *with respect to p and p' has the form*

$$\begin{array}{ccc}
\dfrac{f_{u,r}(q^p)}{f_{u,r}(q)} & \overset{(1)}{\equiv} & \dfrac{f_{u,p}(q^r)}{f_{u,p}(q)} \\
\cdots & \cdots & \cdots \\
\dfrac{f_{u_{p,j},r}(q^p)}{f_{u_{p,j},r}(q)} & \overset{(j)}{\equiv} & \dfrac{f_{u_{p,j},p}(q^r)}{f_{u_{p,j},p}(q)} \\
\cdots & \cdots & \cdots \\
Q_{p,r}(q) & = & Q_{p,r}(q).
\end{array}$$

In other words, the reduced form of EFE(1) *with respect to p and p' is also its super-reduced form.*

(b) *Let $u_{p,e_{1,r}}$ be the value of the level $e_{1,r}$ where $e_{1,r}$ is the smallest level of $f_p(q)$ such that r divides $u_{p,e_{1,r}}$. Let b_r be the highest power of r dividing $u_{p,e_{1,r}}$. Then the reduced form of* EFE(1) *with respect to p and r has the form*

$$\begin{array}{ccc}
\dfrac{f_{u,r}(q^p)}{f_{u,r}(q)} & \overset{(1)}{\longleftrightarrow} & \dfrac{f_{u,p}(q^r)}{f_{u,p}(q)} \\
\cdots & \cdots & \cdots \\
\dfrac{f_{u_{p,e_{1,r}-1},r}(q^p)}{f_{u_{p,e_{1,r}-1},r}(q)} & \overset{(e_{1,r}-1)}{\longleftrightarrow} & \dfrac{f_{u_{p,e_{1,r}-1},p}(q^r)}{f_{u_{p,e_{1,r}-1},p}(q)} \\
f_{u_{p,e_{1,r}},p}(q)\dfrac{f_{u_{p,e_{1,r}},r}(q^p)}{f_{u_{p,e_{1,r}},r}(q)} & \overset{(e_{1,r})}{\longleftrightarrow} & f_{u_{p,e_{1,r}},p}\big(q^r\big) \\
\cdots & \cdots & \cdots \\
f_{\frac{u_{p,e_{1,r}}}{r},p}(q)\dfrac{f_{\frac{u_{p,e_{1,r}}}{r},r}(q^p)^{s_{r,e_{1,r}}}}{f_{\frac{u_{p,e_{1,r}}}{r},r}(q)^{s_{r,e_{1,r}}}} & \overset{(e_{2,r})}{\longleftrightarrow} & f_{\frac{u_{p,e_{1,r}}}{r},p}\big(q^r\big) \\
\cdots & \cdots & \cdots \\
f_{\frac{u_{p,e_{1,r}}}{r^2},p}(q)\dfrac{f_{\frac{u_{p,e_{1,r}}}{r^2},r}(q^p)^{s_{r,e_2}}}{f_{\frac{u_{p,e_{1,r}}}{r^2},r}(q)^{s_{r,e_2}}} & \overset{(e_{3,r})}{\longleftrightarrow} & f_{\frac{u_{p,e_{1,r}}}{r^2},p}\big(q^r\big) \\
\cdots & \cdots & \cdots \\
\dfrac{f_{\frac{u_{p,e_{1,r}}}{r^{b_r}},r}(q^p)^{s_{r,e_{b_r}}}}{f_{\frac{u_{p,e_{1,r}}}{r^{b_r}},r}(q)^{s_{r,e_{b_r}}}} & \overset{(e_{b_r,r})}{\longleftrightarrow} & \dfrac{f_{\frac{u_{p,e_{1,r}}}{r^{b_r}},p}(q^r)}{f_{\frac{u_{p,e_{1,r}}}{r^{b_r}},p}(q)} \\
\cdots & \cdots & \cdots \\
Q_{p,r}(q) & = & Q_{p,r}(q)
\end{array}$$

for some bi-levels $e_{1,r},\dots,e_{b_r,r}$ having values $v_{p,r,e_{1,r}},\dots,v_{p,r,e_{b_r,r}}$ which are equal to $\frac{u_{p,e_{1,r}}}{r},\dots,\frac{u_{p,e_{1,r}}}{r^{b_r}}$ correspondingly.

Proof. (a) As discussed earlier, we may assume that $f_{u_{p,j},p}(q)\neq 1$ for all factor(s) $f_{u_{p,j},p}(q)$ in $f_p(q)=\prod_j f_{u_{p,j},p}(q)$. Since p and p' do not divide $v_{p,p',i}$, the value of the bi-level i, for any bi-level i of EFE(1) with respect to p and p', it can be verified that every line (i) of the reduced form of EFE(1) with respect to p and p' has the form

$$\frac{f_{v_{p,p',i},p'}(q^p)^{s_{p',i}}}{f_{v_{p,p',i},p'}(q)^{s_{p',i}}} \overset{(i)}{\longleftrightarrow} \frac{f_{v_{p,p',i},p}(q^{p'})^{s_{p,i}}}{f_{v_{p,p',i},p}(q)^{s_{p,i}}},$$

where either $s_{p,i}=1$ or $s_{p',i}=1$. If $s_{p,i}=1$, then it is straightforward to verify that roots of

$$\frac{f_{v_{p,p',i},p}(q^{p'})^{s_{p,i}}}{f_{v_{p,p',i},p}(q)^{s_{p,i}}}=\frac{f_{v_{p,p',i},p}(q^{p'})}{f_{v_{p,p',i},p}(q)}$$

are primitive $v_{p,p',i}pp'$-roots of unity. Moreover, $\frac{f_{v_{p,p',i},p}(q^{p'})}{f_{v_{p,p',i},p}(q)}$ is the monic factor of

$$f_{p'}(q) f_p\big(q^{p'}\big)$$

whose roots are all the roots of $f_p(q) f_{p'}(q^p)$ which are primitive $v_{p,p',i}pp'$-roots of unity. It can also be verified that $\frac{f_{v_{p,p',i},p'}(q^p)^{s_{p',i}}}{f_{v_{p,p',i},p'}(q)^{s_{p',i}}}$ is the monic factor of

$$f_p(q) f_{p'}\big(q^p\big)$$

whose roots are all the roots of $f_{p'}(q) f_p(q^{p'})$ which are primitive $v_{p,p',i}pp'$-roots of unity. Since

$$f_p(q) f_{p'}\big(q^p\big) = f_{p'}(q) f_p\big(q^{p'}\big),$$

it follows that

$$\frac{f_{v_{p,p',i},p'}(q^p)^{s_{p',i}}}{f_{v_{p,p',i},p'}(q)^{s_{p',i}}} = \frac{f_{v_{p,p',i},p}(q^{p'})}{f_{v_{p,p',i},p}(q)},$$

and thus $s_{p',i} = 1$. By the same argument, if $s_{p',i} = 1$, then $s_{p,i} = 1$. As a result, every bi-level of EFE(1) with respect to p and p' is a level of $f_p(q)$, i.e., if $v_{p,p',i}$ is the value of some bi-level i of EFE(1) with respect to p and p', then $v_{p,p',i} = u_{p,j}$ for some level j of $f_p(q)$. Therefore, the result follows.

(b) If $e_{1,r} > 1$, then p and r do not divide $v_{p,r,i}$ for $i = 1, \ldots, e_{1,r} - 1$. As a result, an argument similar to that of part (a) above can be applied, and thus line (1) through line $(u_{p,e_{1,r}})$ has the form

$$\begin{array}{ccc} \dfrac{f_{u,r}(q^p)}{f_{u,r}(q)} & \overset{(1)}{\longleftrightarrow} & \dfrac{f_{u,p}(q^r)}{f_{u,p}(q)} \\ \cdots & \cdots & \cdots \\ \dfrac{f_{u_{p,e_{1,r}-1},r}(q^p)}{f_{u_{p,e_{1,r}-1},r}(q)} & \overset{(e_{1,r}-1)}{\longleftrightarrow} & \dfrac{f_{u_{p,e_{1,r}-1},p}(q^r)}{f_{u_{p,e_{1,r}-1},p}(q)}. \end{array}$$

It is also straightforward to verify that $\overset{(i)}{\longleftrightarrow}$ can be replaced by $\overset{(i)}{=}$ for $i = 1, \ldots, e_{1,r}$. As a result, it can be verified that

$$\frac{f_p(q)}{\prod_{1 \leqslant i < e_{1,r}} f_{v_{p,r,i},p}(q)} = \frac{f_p(q)}{\prod_{1 \leqslant i < e_{1,r}} f_{u_{p,i},p}(q)}$$

and

$$\frac{f_r(q)}{\prod_{1 \leqslant i < e_{1,r}} f_{v_{p,r,i},r}(q)} = \frac{f_r(q)}{\prod_{1 \leqslant i < e_{1,r}} f_{u_{p,i},r}(q)}$$

satisfy Functional Equation (1). Consequently, we may assume that $e_{1,r} = 1$. Therefore, we need to show that the reduced form of EFE(1) with respect to p and r has the form

$$\begin{array}{ccc} f_{u,p}(q) \dfrac{f_{u,r}(q^p)}{f_{u,r}(q)} & \overset{(1)}{\longleftrightarrow} & f_{u,p}\big(q^r\big) \\ \cdots & \cdots & \cdots \end{array}$$

$$\begin{array}{ccc}
f_{\frac{u}{r},p}(q)\dfrac{f_{\frac{u}{r},r}(q^p)^{s_{r,e_{2,r}}}}{f_{\frac{u}{r},r}(q)^{s_{r,e_{2,r}}}} & \overset{(e_{2,r})}{\longleftrightarrow} & f_{\frac{u}{r},p}\big(q^r\big)\\
\cdots & \cdots & \cdots\\
f_{\frac{u}{r^2},p}(q)\dfrac{f_{\frac{u}{r^2},r}(q^p)^{s_{r,e_{3,r}}}}{f_{\frac{u}{r^2},r}(q)^{s_{r,k_{2,r}}}} & \overset{(e_{3,r})}{\longleftrightarrow} & f_{\frac{u}{r^2},p}\big(q^r\big)\\
\cdots & \cdots & \cdots\\
\dfrac{f_{\frac{u}{r^{b_r}},r}(q^p)^{s_{r,e_{b_r+1,r}}}}{f_{\frac{u}{r^{b_r}},r}(q)^{s_{r,e_{b_r+1,r}}}} & \overset{(e_{b_r+1,r})}{\longleftrightarrow} & \dfrac{f_{\frac{u}{r^{b_r}},p}(q^r)}{f_{\frac{u}{r^{b_r}},p}(q)}\\
\cdots & \cdots & \cdots\\
Q_{p,r}(q) & = & Q_{p,r}(q)
\end{array}$$

where $e_{2,r},\dots,e_{b_r+1,r}$ are the bi-levels of EFE(1) with respect to p and r having values $\frac{u}{r},\dots,\frac{u}{r^{b_r}}$ correspondingly.

Consider the reduced form of EFE(1) with respect to p and r:

$$\begin{array}{ccc}
f_{v_{p,r,1},p}(q)^{s_{p,1}\delta_{r,1}}\dfrac{f_{v_{p,r,1},r}(q^p)^{s_{r,1}}}{f_{v_{p,r,1},r}(q)^{s_{v_{r,1}}(1-\delta_{p,1})}} & \overset{(1)}{\longleftrightarrow} & f_{v_{p,r,1},r}(q)^{s_{v_{r,1}}\delta_{p,1}}\dfrac{f_{v_{p,r,1},p_0}(q^r)^{s_{v_{p,1}}}}{f_{v_{p,r,1},p}(q)^{s_{v_{p,1}}(1-\delta_{r,1})}}\\
\cdots & \cdots & \cdots\\
f_{v_{p,r,i},p}(q)^{s_{p,i}\delta_{r,i}}\dfrac{f_{v_{p,r,i},r}(q^p)^{s_{r,i}}}{f_{v_{p,r,i},r}(q)^{s_{v_{r,i}}(1-\delta_{p,i})}} & \overset{(i)}{\longleftrightarrow} & f_{v_{p,r,i},r}(q)^{s_{v_{r,i}}\delta_{p,i}}\dfrac{f_{v_{p,r,i},p_0}(q^r)^{s_{v_{p,i}}}}{f_{v_{p,r,i},p}(q)^{s_{v_{p,i}}(1-\delta_{r,i})}}\\
\cdots & \cdots & \cdots\\
Q_{p,r}(q) & = & Q_{p,r}(q).
\end{array}$$

By Key Proposition 1′, $s_{v_{p,1}}=s_{v_{r,1}}=1$. Since p does not divide $u:=v_{p,r,1}$ and r divides u by assumption, $\delta_{p,1}=0$ and $\delta_{r,1}=1$. Thus the first line of the reduced form of EFE(1) must be

$$f_{u,p}(q)\frac{f_{u,r}(q^p)}{f_{u,r}(q)}\overset{(1)}{\longleftrightarrow} f_{u,p}\big(q^r\big).$$

As a result, there must exist a collection of bi-levels $\mathcal{L}:=\{k_1,\dots,k_n\}$ such that $f_{u,p}(q)$ divides $\prod_{k_j\in\mathcal{L}} f_{v_{p,r,k_j},r}(q)^{s_{v_{r,k_j}}} f_{v_{p,r,k_j},p}(q^r)^{s_{v_{p,k_j}}}$. We suppose that $\mathcal{L}$ is a minimal such set. Since $f_{u,p}(q)=f_{v_{p,r,1},r}(q)\neq 1$, it possesses at least one root, say α, which is a primitive up-root of unity. Then α must be a root of $f_{v_{p,r,k_j},r}(q)^{s_{v_{r,k_j}}} f_{v_{p,r,k_j},p}(q^r)^{s_{v_{p,k_j}}}$ for some bi-level $k_\eta\in\mathcal{L}$. Since p does not divide v_{p,r,k_j} for any k_j by definition of p, α must be a root of $f_{v_{p,r,k_\eta},p}(q^r)^{s_{v_{p,k_\eta}}}$ and thus $s_{v_{p,k_\eta}}=1$. Therefore α is either a primitive $v_{p,r,k_{\eta,r}}p$-root of unity or a primitive $v_{p,r,k_\eta}pr$-root of unity. Since $u>v_{p,r,k_\eta}$, $up>v_{p,r,k_\eta}p$. Therefore, α must be a primitive $v_{p,r,k_\eta}pr$-root of unity. Hence $u=v_{p,r,k_\eta}r$ and thus $v_{p,r,k_\eta}=\frac{u}{r}$. Since α is an arbitrary root of $f_{u,p}(q)$, every root of $f_{u,p}(q)$ must be a root of $f_{v_{p,r,k_\eta},p}(q^r)$. Thus $f_{u,p}(q)$ divides $f_{v_{p,r,k_\eta},p}(q^r)$. Therefore by the minimality of $\mathcal{L}$, $\mathcal{L}=\{k_\eta\}$. We may assume that $\eta=1$ thus $\mathcal{L}=\{k_1\}$ and $v_{p,r,k_1}=\frac{u}{r}$. Thus line (k_1) of EFE(1) has the form

$$f_{\frac{u}{r},p}(q)^{\delta_{r,k_1}}\frac{f_{\frac{u}{r},r}(q^p)^{s_{r,k_1}}}{f_{\frac{u}{r},r}(q)^{s_{r,k_1}}}\overset{(k_1)}{\longleftrightarrow}\frac{f_{\frac{u}{r},p}(q^r)}{f_{\frac{u}{r},p}(q)^{(1-\delta_{r,k_1})}}.$$

If $b_r = 1$, then r does not divide $\frac{u}{r}$. Hence $\delta_{r,k_1} = 0$. Thus line (k_1) of the reduced form of EFE(1) with respect to p and r has the form

$$\frac{f_{\frac{u}{r},r}(q^p)^{s_{r,k_1}}}{f_{\frac{u}{r},r}(q)^{s_{r,k_1}}} \overset{(k_1)}{\longleftrightarrow} \frac{f_{\frac{u}{r},p}(q^r)}{f_{\frac{u}{r},p}(q)}.$$

If $b_r > 1$, then r divides $\frac{u}{r}$. Hence $\delta_{r,k_1} = 1$ and line (k_1) of the reduced form of EFE(1) with respect to p and r has the form

$$f_{\frac{u}{r},p}(q)\frac{f_{\frac{u}{r},r}(q^p)^{s_{r,k_1}}}{f_{\frac{u}{r},r}(q)^{s_{r,k_1}}} \overset{(k_1)}{\longleftrightarrow} f_{\frac{u}{r},p}\big(q^r\big).$$

Now repeat the process above until we reach the line (k_{b_r}) of EFE(1) which must have the form

$$f_{\frac{u}{r^{b_r}},p}(q)^{\delta_{r,k_{b_r}}}\frac{f_{\frac{u}{r^{b_r}},r}(q^p)^{s_{r,k_{b_r}}}}{f_{\frac{u}{r^{b_r}},r}(q)^{s_{r,k_{b_r}}}} \overset{(k_{b_r})}{\longleftrightarrow} \frac{f_{\frac{u}{r^{b_r}},p}(q^r)}{f_{\frac{u}{r^{b_r}},p}(q)^{(1-\delta_{r,k_{b_r}})}}.$$

Since r does not divide $\frac{u}{r^{b_r}}$ by definition of b_r, it follows that $\delta_{r,k_{b_r}} = 0$ and thus line (k_{b_r}) of the reduced form of EFE(1) must have the form

$$\frac{f_{\frac{u}{r^{b_r}},r}(q^p)^{s_{r,k_{b_r}}}}{f_{\frac{u}{r^{b_r}},r}(q)^{s_{r,k_{b_r}}}} \overset{(k_{b_r})}{\longleftrightarrow} \frac{f_{\frac{u}{r^{b_r}},p}(q^r)}{f_{\frac{u}{r^{b_r}},p}(q)}.$$

By replacing $k_1, \ldots, k_{b_r}$ by $e_{2,r}, \ldots, e_{b_r+1,r}$ correspondingly to indicate the dependence of these bi-levels on r, the proof of Key Proposition 2 is complete. □

Proposition 3.23 *(Key Proposition 3). Let Γ be a sequence of polynomials satisfying the full hypothesis of Theorem* 2.1 *whose field of coefficients is of characteristic zero and strictly contains $\mathbb{Q}$.*

(1) *Let $V := \{v_{x,y,i}\}$ where $v_{x,y,i}$ is the value of each bi-level i of* EFE(1) *with respect to any primes x and y for which either $s_{x,i}$ or $s_{y,i}$ is* 1. *If $\mathcal{U}$ is the set of all distinct prime factors of any element of V, then $\mathcal{U}$ is a finite set. Therefore there exists a prime greater than any element of $\mathcal{U}$.*

(2) *Let z be a prime which is greater than any element of $\mathcal{U}$ and r be any prime. If $k_{z,r}$ is the smallest positive integer such that $f_{v_{z,r,k_{z,r}},z}(q)$ (resp. $f_{v_{z,r,k_{z,r}},r}(q)$) is a polynomial not contained in $\mathbb{Q}[q]$, then $k_{z,r}$ is also the smallest positive integer such that $f_{v_{z,r,k_{z,r}},r}(q)$ (resp. $f_{v_{z,r,k_{z,r}},z}(q)$) is a polynomial not contained in $\mathbb{Q}[q]$.*

(3) *There exists a positive integer L such that if z is a prime greater than any element of $\mathcal{U}$, r any prime and $k_{z,r}$ as in* (2), *then $s_{z,k_{z,r}} = s_{r,k_{z,r}} = 1$ and $v_{z,r,k_{z,r}} = L$.*

Proof. Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a sequence of polynomials satisfying the hypothesis of this proposition. Thus $\deg(f_n(q)) = t_\Gamma(n-1)$, which means that $f_n(q) \neq 1$ for all n in $\mathbb{N}$ and the set of primes P associated to the support of Γ contains *all* prime numbers. Let $\Gamma_P := \{f_{p_i}(q) \mid p_i \in P = \{2, 3, 5, \ldots\}\}$. We write $f_{p_i}(q) = \prod_{u_{p_i,j} > u_{p_i,j+1}} f_{u_{p_i,j},p_i}(q)$ with $f_{u_{p_i,j},p_i}(q)$ being the factor all of whose roots are primitive $u_{p_i,j}p_i$-roots of unity. Let $\mathcal{J}_{p_i} := \{j\}$ be the set which consists of all levels j where $f_{u_{p_i,j},p_i}(q)$ is not a polynomial in $\mathbb{Q}[q]$. As the field of coefficients of Γ strictly contains $\mathbb{Q}$, $\mathcal{J}_{p_i}$ must be nonempty for at least one p_i since if $\mathcal{J}_{p_i}$ is empty for all p_i, then the field of coefficients of Γ is $\mathbb{Q}$. Therefore, we may assume from now on that there exists a prime, say p_c, such that $\mathcal{J}_{p_c}$ is nonempty.

(1) Let p_n and p_m be any two primes. Let $v_{p_n,p_m,1}$ be the value of the bi-level 1 of EFE(1) with respect to p_n and p_m. Then $v_{p_n,p_m,1} = u$ by Key Proposition 1′. Note that

$$v_{p_n,p_m,1} \geqslant v_{p_n,p_m,i}$$

for any bi-level $i \geqslant 1$. Let s be any prime in $\mathcal{U}$, then there exist two primes, say x and y, and a bi-level l of EFE(1) with respect to x and y such that s divides $v_{x,y,l}$. As a result,

$$s \leqslant v_{x,y,l} \leqslant v_{x,y,1} = u.$$

Since there is only a finite number of primes less than or equal to u,

$$|\mathcal{U}| < \infty.$$

(2) Let z be a prime greater than any element of $\mathcal{U}$. Without loss of generality, we may assume that $z = p$ where p is the prime chosen in part (1) above. It is immediate from the definition of p that it does not divide $v_{p_i,p_j,l}$ for any $v_{p_i,p_j,l}$ appearing in EFE(1) of Γ with respect to any primes p_i and p_j.

Lemma 3.24. *Let $\mathcal{J}_p = \{j\}$ be the collection of all levels of $f_p(q)$ such that the coefficients of $f_{u_j,p}(q)$ are not properly contained in $\mathbb{Q}$. Then $\mathcal{J}_p \neq \emptyset$. Furthermore, if k is the smallest integer such that the coefficients of $f_{v_{p,p_c,k},p}(q)$ are not properly contained in $\mathbb{Q}$, then k is also the smallest integer such that the coefficients of $f_{v_{p,r,k},p_c}(q)$ are not properly contained in $\mathbb{Q}$.*

Proof. Let p be the prime chosen above and p_c be the prime for which we assume that $\mathcal{J}_{p_c} \neq \emptyset$ earlier. There are two cases to consider:

(A) p_c is not in $\mathcal{U}$.
(B) p_c is in $\mathcal{U}$.

Case (A): We suppose that p_c is not in $\mathcal{U}$. Then the reduced form of EFE(1) with respect to p and p_c has the form

$$\begin{array}{ccc}
\dfrac{f_{v_{p,p_c,1},p_c}(q^p)}{f_{v_{p,p_c,1},p_c}(q)} & \overset{(1)}{=} & \dfrac{f_{v_{p,p_c,1},p}(q^{p_c})}{f_{v_{p,p_c,1},p}(q)} \\
\cdots & \cdots & \cdots \\
\dfrac{f_{v_{p,p_c,k},p_c}(q^s)}{f_{v_{p,p_c,k},p_c}(q)} & \overset{(k)}{=} & \dfrac{f_{v_{p,p_c,k},p}(q^{p_c})}{f_{v_{p,p_c,k},p}(q)} \\
\cdots & \cdots & \cdots \\
Q_{p,p_c}(q) & = & Q_{p,p_c}(q)
\end{array}$$

by part (a) of Key Proposition 2. Also, all the rational expressions are actually polynomials by Key Proposition 1′.

Suppose k is the smallest integer such that the coefficients of $f_{v_{p,p_c,k},p_c}(q)$ are not properly contained in $\mathbb{Q}$.

If $k > 1$, then the coefficients of $f_{v_{p,p_c,1},p_c}(q)$ are contained in $\mathbb{Q}$. Thus

$$f_{v_{p,p_c,1},p_c}(q) = P_{v_{p,p_c,1},p_c}(q)^n$$

for some positive integer n. It follows that

$$\frac{f_{v_{p,p_c,1},p_c}(q^p)}{f_{v_{p,p_c,1},p_c}(q)} = \frac{P_{v_{p,p_c,1},p_c}(q^p)^n}{P_{v_{p,p_c,1},p_c}(q)^n} = P_{v_{p,p_c,1}pp_c}(q)^n,$$

where $P_{v_{p,p_c,1}pp_c}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ of order $v_{p,p_c,1}pp_c$. As a result,

$$\frac{f_{v_{p,p_c,1},p}(q^{p_c})}{f_{v_{p,p_c,1},p}(q)} = P_{v_{p,p_c,1}pp_c}(q)^n.$$

Therefore $f_{v_{p,p_c,1},p}(q) = P_{v_{p,p_c,1},p}(q)^n$ where $P_{v_{p,p_c,1},p}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ of order $v_{p,p_c,1}p$, i.e., the coefficients of $f_{v_{p,p_c,1},p}(q)$ are also contained in $\mathbb{Q}$. As this argument can be applied to $\frac{f_{v_{p,p_c,i},p_c}(q^p)}{f_{v_{p,p_c,i},p_c}(q)}$ and $\frac{f_{v_{p,p_c,i},p}(q^{p_c})}{f_{v_{p,p_c,i},p}(q)}$ for each $i \in \{1,\dots,k-1\}$, it follows that the coefficients of each polynomial in the collection

$$\left\{ f_{v_{p,p_c,i},p}(q) \;\middle|\; 1 \leqslant i \leqslant k-1 \right\}$$

are contained in $\mathbb{Q}$.

Let us suppose that the coefficients of $f_{v_{p,p_c,k},p}(q)$ are properly contained in $\mathbb{Q}$. It can be verified that

$$f_{v_{p,p_c,k},p}(q) = P_{v_{p,p_c,k},p}(q)^{n_k}$$

for some positive integer n_k. Hence,

$$\frac{f_{v_{p,p_c,k},p}(q^{p_c})}{f_{v_{p,p_c,k},p}(q)} = \frac{P_{v_{p,p_c,k},p}(q^{p_c})^{n_k}}{P_{v_{p,p_c,k},p}(q)^{n_k}} = P_{v_{p,p_c,k}p_cp}(q)^{n_k}$$

where $P_{v_{p,p_c,k}p_cp}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ of order $v_{p,p_c,k}p_cp$. Therefore,

$$\frac{f_{v_{p,p_c,k},p_c}(q^p)}{f_{v_{p,p_c,k},p_c}(q)} = \frac{P_{v_{p,p_c,k},p}(q^{p_c})^{n_k}}{P_{v_{p,p_c,k},p}(q)^{n_k}} = P_{v_{p,p_c,k}p_cp}(q)^{n_k}.$$

However, it can be verified that

$$\frac{P_{v_{p,p_c,k},p_c}(q^p)^{n_k}}{P_{v_{p,p_c,k},p_c}(q)^{n_k}} = P_{v_{p,p_c,k}p_cp}(q)^{n_k}.$$

It is straightforward to verify from this that

$$f_{v_{p,p_c,k},p_c}(q) = P_{v_{p,p_c,k},p_c}(q)^{n_k}.$$

Hence the coefficients $f_{v_{p,p_c,k},p_c}(q)$ are properly contained in $\mathbb{Q}$. This contradicts the definition of k. As a result, $\mathcal{J}_p \supseteq \{k\}$ and k is also the smallest positive integer such that the coefficients of $f_{v_{p,p_c,k},p}(q)$ are not properly contained in $\mathbb{Q}$.

Case (B): Now suppose that p_c is in $\mathcal{U}$. Again consider the reduced form of EFE(1) with respect to p and p_c. Let g be the smallest positive integer such that p_c divides $v_{p,p_c,g}$. It can be verified that the reduced form of EFE(1) must have the form:

$$\begin{array}{ccc}
\dfrac{f_{v_{p,p_c,1},p_c}(q^p)}{f_{v_{p,p_c,1},p_c}(q)} & \overset{(1)}{=} & \dfrac{f_{v_{p,p_c,1},p}(q^{p_c})}{f_{v_{p,p_c,1},p}(q)} \\
\cdots & \cdots & \cdots \\
\dfrac{f_{v_{p,p_c,g-1},p_c}(q^p)}{f_{v_{p,p_c,g-1},p_c}(q)} & \overset{(g-1)}{=} & \dfrac{f_{v_{p,p_c,g-1},p}(q^{p_c})}{f_{v_{p,p_c,g-1},p}(q)} \\
f_{v_{p,p_c,g},p}(q)\dfrac{f_{v_{p,p_c,g},p_c}(q^p)}{f_{v_{p,p_c,g},p_c}(q)} & \overset{(g)}{\longleftrightarrow} & f_{v_{p,p_c,g},p}\big(q^{p_c}\big) \\
\cdots & \cdots & \cdots \\
Q_{p,p_c}(q) & = & Q_{p,p_c}(q).
\end{array}$$

In particular $s_{p,i} = s_{r,i} = 1$ for $i \in \{1, \ldots, g\}$, i.e. $f_{v_{p,p_c,i},p}(q) \neq 1$ and $f_{v_{p,p_c,i},p_c}(q) \neq 1$ for $i \in \{1, \ldots, g\}$. If $k < g$, then the argument in Case (A) is applied and the result follows. Thus let us assume otherwise.

Claim. *There exists a level, say l_g, such that $f_{v_{p,p_c,g},p}(q)$ divides $\frac{f_{v_{p,p_c,l_g},p}(q^{p_c})}{f_{v_{p,p_c,l_g},p}(q)^{1-\delta_{p,l_g}}}$ where $\delta_{p,l_g} = 1$ if p_c divides $v_{p,p_c,g}$ and is equal to 0 otherwise. Furthermore, l_g is unique and $l_g > g$.*

Proof. From the reduced form of EFE(1) above, $f_{v_{p,p_c,g},p}(q) \neq 1$ and thus has at least one root, say α, which is a primitive $v_{p,p_c,g}p$-root of unity. Again from the reduced form above, α must be a root of exactly one polynomial on the right-hand side of $\overset{(l)}{\longleftrightarrow}$ for some bi-level l, where the uniqueness of such a polynomial comes from the fact that the roots of each polynomial appearing on the right-hand column of the reduced form of EFE(1) above are primitive roots of unity of different orders. Hence, $s_{p,l} = 1$. Thus line (l) has the form

$$f_{v_{p,p_c,l},p}(q)^{\delta_{p,l}}\frac{f_{v_{p,p_c,l},p_c}(q^p)^{s_{p_c,l}}}{f_{v_{p,p_c,l},p_c}(q)^{s_{p_c,l}}} \overset{(l)}{\longleftrightarrow} \frac{f_{v_{p,p_c,l},p}(q^{p_c})}{f_{v_{p,p_c,l},p}(q)^{1-\delta_{p,l}}}$$

where $\delta_{p,l} = 1$ if p_c divides $v_{p,p_c,g}$ and equal to 0 otherwise. Hence, α must be a root of $\frac{f_{v_{p,p_c,l},p}(q^{p_c})}{f_{v_{p,p_c,l},p}(q)^{1-\delta_{p,l}}}$. Since every root of $f_{v_{p,p_c,l},p}(q^{p_c})$ is a primitive $v_{p,p_c,l}pp_c$-root of unity or a primitive $v_{p,p_c,l}p$-root of unity depending on whether p_c divides $v_{p,p_c,l}$ or not respectively, every root of $\frac{f_{v_{p,p_c,l},p}(q^{p_c})}{f_{v_{p,p_c,l},p}(q)^{1-\delta_{p,l}}}$ must be a primitive $v_{p,p_c,l}pp_c$-root of unity by our prior analysis. Hence,

$$v_{p,p_c,g}p = v_{p,p_c,l}pp_c,$$

which is equivalent to

$$v_{p,p_c,l} = \frac{v_{p,p_c,g}}{p_c}.$$

Thus $v_{p,p_c,l}$ is determined uniquely by p_c and $v_{p,p_c,g}$. As the prime p_c is fixed, we denote l by l_g to signify the dependency on g. Since this is true for every root of $f_{v_{p,p_c,g},p}(q)$, $f_{v_{p,p_c,g},p}(q)$ must divide $\frac{f_{v_{p,p_c,l},p}(q^{p_c})}{f_{v_{p,p_c,l},p}(q)^{1-\delta_{p,l}}}$ and thus the claim follows. □

Our goal is to produce the k-super-reduced form of EFE(1) with respect to p and p_c because we can then use an argument similar to part (1) to reach the desired conclusion. First we rewrite the reduced form of EFE(1) above by moving the factor $f_{v_{p,p_c,g},p}(q)$ to the line (l_g) as follows.

$$
\begin{array}{ccc}
\dfrac{f_{v_{p,p_c,1},p_c}(q^p)}{f_{v_{p,p_c,1},p_c}(q)} & \overset{(1)}{=} & \dfrac{f_{v_{p,p_c,1},p}(q^{p_c})}{f_{v_{p,p_c,1},p}(q)} \\
\cdots & \cdots & \cdots \\
\dfrac{f_{v_{p,p_c,g-1},p_c}(q^p)}{f_{v_{p,p_c,k-1},p_c}(q)} & \overset{(g-1)}{=} & \dfrac{f_{v_{p,p_c,g-1},p}(q^{p_c})}{f_{v_{p,p_c,g-1},p}(q)} \\
\dfrac{f_{v_{p,p_c,g},p_c}(q^p)}{f_{v_{p,p_c,g},p_c}(q)} & \overset{(g)}{=} & f_{v_{p,p_c,g},p}\big(q^{p_c}\big) \\
\cdots & \cdots & \cdots \\
\big(f_{v_{p,p_c,l_g},p}(q)\big)^{\delta_{p,l_g}} \dfrac{(f_{v_{p,p_c,g},p}(q))f_{v_{p,p_c,l_g},p_c}(q^p)}{f_{v_{p,p_c,l_g},p_c}(q)} & \overset{(l_g)}{\longleftrightarrow} & \dfrac{f_{v_{p,p_c,l_g},p}(q^{p_c})}{(f_{v_{p,p_c,l_g},p}(q))^{1-\delta_{p,l_g}}} \\
\cdots & \cdots & \cdots \\
Q_{p,p_c}(q) & = & Q_{p,p_c}(q).
\end{array}
$$

As a result, we obtain the g-super-reduced form of EFE(1) with respect to p and p_c. Moreover, we also have

$$
\frac{(f_{v_{p,p_c,g},p}(q))f_{v_{p,p_c,l_g},p_c}(q^p)}{f_{v_{p,p_c,l_g},p_c}(q)} = \frac{f_{v_{p,p_c,l_g},p}(q^{p_c})}{(f_{v_{p,p_c,l_g},p}(q))^{1-\delta_{p,l_g}}}
$$

by the claim above (this allows us to repeat the moving factor process, applied at line (g) above, to line l_g if $l_g < k$ to obtain the k-super-reduced form).

Note that if $\delta_{p,l_g} = 1$, then it is straightforward to verify that $\overset{(l_g)}{\longleftrightarrow}$ becomes $\overset{(l_g)}{=}$, i.e. equality occurs at line (l_g) since the polynomials on LHS and RHS of $\overset{(l_g)}{\longleftrightarrow}$ are the only factors of $f_p(q)f_{p_c}(q^p)$ and $f_{p_c}(q)f_p(q^{p_c})$ respectively having the property that their roots are exactly all the primitive $v_{p,p_c,l_g}p_cp$-roots of unity which are roots of $f_p(q)f_{p_c}(q^p)$ and $f_{p_c}(q)f_p(q^{p_c})$ respectively.

Now let us repeat this process starting at line $(g+1)$:

(i) If $g+1 \neq l_g$, i.e., $g+1 < l_g$, then line $(g+1)$ has the form

$$
f_{v_{p,p_c,g+1},p}(q)^{\delta_{p,g+1}} \frac{f_{v_{p,p_c,g+1},p_c}(q^p)}{f_{v_{p,p_c,g+1},p_c}(q)} \overset{(g+1)}{\longleftrightarrow} \frac{f_{v_{p,p_c,g+1},p}(q^{p_c})}{f_{v_{p,p_c,g+1},p}(q)^{1-\delta_{p,g+1}}}
$$

where $\delta_{p,g+1} = 1$ if p_c divides $v_{p,p_c,g+1}$ and is equal to 0 otherwise.

If p_c does not divide $v_{p,p_c,g+1}$, then $\overset{(g+1)}{\longleftrightarrow}$ can be replaced by $\overset{(g+1)}{=}$ and line $(g+1)$ has the form

$$
\frac{f_{v_{p,p_c,g+1},p_c}(q^p)}{f_{v_{p,p_c,g+1},p_c}(q)} \overset{(g+1)}{=} \frac{f_{v_{p,p_c,g+1},p}(q^{p_c})}{f_{v_{p,p_c,g+1},p}(q)}.
$$

Thus, we obtain the $(g+1)$-super-reduced form of EFE(1) with respect to p and p_c. Therefore, if $k \geqslant g+1$, then the result follows from Case (A) if p_c does not divide $v_{p,p_c,g+1}$. If $k > g+1$, then we move on to the next line, namely line $(g+2)$.

If p_c divides $v_{p,p_c,g+1}$, then for the same reason as in line (g) above, there exists a unique level l_{g+1} such that $f_{v_{p,p_c,g+1},p}(q)$ divides $f_{v_{p,p_c,l_{g+1}},p}(q^{p_c})$. After being rewritten as in line l_g, line $(g+1)$ and line (l_{g+1}) have the form

$$
\frac{f_{v_{p,p_c,g+1},p_c}(q^p)}{f_{v_{p,p_c,g+1},p_c}(q)} \overset{(g+1)}{=} f_{v_{p,p_c,g+1},p}\big(q^{p_c}\big)
$$

and

$$\left(f_{v_{p,p_c,l_{g+1}},p}(q)\right)^{\delta_{p,l_{g+1}}}\frac{(f_{v_{p,p_c,g+1},p}(q))f_{v_{p,p_c,l_{g+1}},p_c}(q^p)}{f_{v_{p,p_c,l_{g+1}},p_c}(q)}\overset{(l_{g+1})}{\longleftrightarrow}\frac{f_{v_{p,p_c,l_{g+1}},p}(q^{p_c})}{(f_{v_{p,p_c,l_{g+1}},p}(q))^{1-\delta_{p,l_{g+1}}}}$$

respectively. Thus we obtain the $(g+1)$-super-reduced form of EFE(1) with respect to p and p_c.

Note that $l_{g+1}\neq l_g$ since it can be deduced similarly as in the case of l_g that $l_{g+1}=\frac{v_{p,p_c,g+1}}{p_c}>\frac{v_{p,p_c,g}}{p_c}=l_g$.

(ii) If $g+1=l_g$, then there are two cases: If $\delta_{p,l_g}=0$, then $\overset{(l_g)}{\longleftrightarrow}$ becomes $\overset{(l_g)}{=}$ as discussed above and we move on to the next line. If $\delta_{p,l_g}=1$, then line (l_g) has the form

$$\left(f_{v_{p,p_c,l_g},p}(q)\right)\frac{(f_{v_{p,p_c,g},p}(q))f_{v_{p,p_c,l_g},p_c}(q^p)}{f_{v_{p,p_c,l_g},p_c}(q)}\overset{(l_g)}{\longleftrightarrow}f_{v_{p,p_c,l_g},p}\left(q^{p_c}\right).$$

Now we apply the same argument as for line (g) earlier to this line which then transforms it into

$$\frac{(f_{v_{p,p_c,g},p}(q))f_{v_{p,p_c,l_g},p_c}(q^p)}{f_{v_{p,p_c,l_g},p_c}(q)}\overset{(l_g)}{=}f_{v_{p,p_c,l_g},p}\left(q^{p_c}\right).$$

We repeat this process again to all subsequent lines starting at line $(g+2)$ and so forth. It can be verified that this process allows us to replace $\overset{(i)}{\longleftrightarrow}$ by $\overset{(i)}{=}$ at every bi-level $i\geqslant 1$ in the reduced form of EFE(1) with respect to p and p_c. In particular, it allows us to produce the k-super-reduced form of EFE(1) with respect to p and p_c.

As $g\leqslant k$ by assumption, it can be deduced, using the same argument as in Case (A) above, that all the polynomials $f_{v_{p,p_c,1},p}(q),\ldots,f_{v_{p,p_c,g-1},p}(q)$ have coefficients contained in $\mathbb{Q}$.

By using the k-super-reduced form of EFE(1) with respect to p and p_c as well as the facts

- $\frac{f_{v_{p,p_c,g},p_c}(q^p)}{f_{v_{p,p_c,g},p_c}(q)}\in\mathbb{Q}[q]$ if and only if $f_{v_{p,p_c,g},p_c}(q)\in\mathbb{Q}[q]$ and
- $f_{v_{p,p_c,g},p}(q^{p_c})\in\mathbb{Q}[q]$ if and only if $f_{v_{p,p_c,g},p}(q)\in\mathbb{Q}[q]$,

we verify below that the lemma follows if we prove the following statements:

(a) If $g\leqslant k$, then $\frac{f_{v_{p,p_c,g},p_c}(q^p)}{f_{v_{p,p_c,g},p_c}(q)}$ has coefficients properly contained in $\mathbb{Q}$ if and only if $f_{v_{p,p_c,g},p}(q^{p_c})$ does.

(b) If $l_g\leqslant k$, then $\frac{(f_{v_{p,p_c,g},p}(q))f_{v_{p,p_c,l_g},p_c}(q^p)}{f_{v_{p,p_c,l_g},p_c}(q)}$ has coefficients properly contained in $\mathbb{Q}$ if and only if $\frac{f_{v_{p,p_c,l_g},p_c}(q^p)}{f_{v_{p,p_c,l_g},p_c}(q)}$ does.

If $g<k$, then the coefficients of $f_{v_{p,p_c,g},p_c}(q)$ are properly contained in $\mathbb{Q}$. It follows that $f_{v_{p,p_c,g},p_c}(q)=P_{v_{p,p_c,g},p_c}(q)^{n_g}$ for some positive integer n_g, where $P_{v_{p,p_c,g},p_c}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ of order $v_{p,p_c,g}p_c$. Hence $\frac{f_{v_{p,p_c,g},p_c}(q^p)}{f_{v_{p,p_c,g},p_c}(q)}=P_{v_{p,p_c,g}pp_c}(q)^{n_g}$ where $P_{v_{p,p_c,g}pp_c}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ of order $v_{p,p_c,g}pp_c$. As $\frac{f_{v_{p,p_c,g},p_c}(q^p)}{f_{v_{p,p_c,g},p_c}(q)}=f_{v_{p,p_c,g},p}(q^{p_c})$, $f_{v_{p,p_c,g},p}(q^{p_c})=P_{v_{p,p_c,g}pp_c}(q)^{n_g}$. Hence the coefficients of $f_{v_{p,p_c,g},p}(q^{p_c})$ and thus those of $f_{v_{p,p_c,g},p}(q)$ are properly contained in $\mathbb{Q}$. If $g=k$, then the coefficients of $f_{v_{p,p_c,g},p_c}(q)$ are not properly contained in $\mathbb{Q}$. Hence there exists a nonnegative integer n_g such that $P_{v_{p,p_c,g},p_c}(q)^{n_g+1}$ does not divide $f_{v_{p,p_c,g},p_c}(q)$ but $P_{v_{p,p_c,g},p_c}(q)^{n_g}$ properly divides $f_{v_{p,p_c,g},p_c}(q)$.

It can be verified then that $P_{v_{p,p_c,g}pp_c}(q)^{n_g+1}$ does not divide $\frac{f_{v_{p,p_c,g},p_c}(q^p)}{f_{v_{p,p_c,g},p_c}(q)}$ but $P_{v_{p,p_c,g}pp_c}(q)^{n_g}$ properly divides $\frac{f_{v_{p,p_c,g},p_c}(q^p)}{f_{v_{p,p_c,g},p_c}(q)}$. Thus $P_{v_{p,p_c,g}pp_c}(q)^{n_g+1}$ does not divide $f_{v_{p,p_c,g},p}(q^{p_c})$ but $P_{v_{p,p_c,g}pp_c}(q)^{n_g}$ properly divides $f_{v_{p,p_c,g},p}(q^{p_c})$. As a result, the coefficients of $f_{v_{p,p_c,g},p}(q^{p_c})$ must not be properly contained in $\mathbb{Q}$. Therefore, the coefficients of $f_{v_{p,p_c,g},p}(q)$ are not properly contained in $\mathbb{Q}$.

If $l_g < k$, then $g < k$. Thus $f_{v_{p,p_c,g},p}(q)$ and $\frac{f_{v_{p,p_c,l_g},p_c}(q^p)}{f_{v_{p,p_c,l_g},p_c}(q)}$ have coefficients properly contained in $\mathbb{Q}$ by the definition of k and the paragraph above. Therefore, the coefficients of $\frac{(f_{v_{p,p_c,g},p}(q))f_{v_{p,p_c,l_g},p_c}(q^p)}{f_{v_{p,p_c,l_g},p_c}(q)}$ are contained in $\mathbb{Q}$ and hence so are the coefficients of $f_{v_{p,p_c,l_g},p}(q^{p_c})$. If $l_g = k$, then $g < k$ and thus all the coefficients of $f_{v_{p,p_c,g},p_c}(q)$ are properly contained in $\mathbb{Q}$. Hence all the coefficients of $\frac{f_{v_{p,p_c,g},p_c}(q^p)}{f_{v_{p,p_c,g},p_c}(q)}$ are properly contained in $\mathbb{Q}$ and thus so are those of $f_{v_{p,p_c,g},p}(q^{p_c})$. Therefore, all the coefficients of $f_{v_{p,p_c,g},p}(q)$ are properly contained in $\mathbb{Q}$. Consequently, all the coefficients of

$$\frac{(f_{v_{p,p_c,g},p}(q))f_{v_{p,p_c,l_g},p_c}(q^p)}{f_{v_{p,p_c,l_g},p_c}(q)} = f_{v_{p,p_c,l_g},p}\left(q^{p_c}\right)$$

are properly contained in $\mathbb{Q}$ if and only if all those of $\frac{f_{v_{p,p_c,l_g},p_c}(q^p)}{f_{v_{p,p_c,l_g},p_c}(q)}$ are. As a result, the coefficients of $f_{v_{p,p_c,l_g},p}(q^{p_c})$ and thus those of $f_{v_{p,p_c,l_g},p}(q) = f_{v_{p,p_c,k},p}(q)$ are not properly contained in $\mathbb{Q}$. Consequently, if $g+1 > k$, then there is nothing to prove. If $g+1 \leqslant k$, we may assume, as discussed in (i) above, that p_c divides $v_{p,p_c,g+1}$. Then the same argument as in line (g) above can be repeated. Therefore, the lemma follows. □

Let s be any prime in $\mathcal{U}$ where $\mathcal{U}$ is defined in part (1). We consider the reduced form of EFE(1) with respect to p and s. It has a similar form to the reduced form of EFE(1) with respect to p and p_c in Case (B). As a result, a similar argument as in Case (B) above, the details of which are left to the readers, holds in this case as well. The proof of (2) is therefore complete.

(3) Again we may assume without loss of generality that $z = p$. Let r be any prime. Let k be the smallest integer such that the coefficients of $f_{v_{p,r,k},p}(q)$ are not properly contained in $\mathbb{Q}$. Then k is also the smallest positive integer such that the coefficients of $f_{v_{p,r,k},r}(q)$ are not properly contained in $\mathbb{Q}$ by part (2). Therefore, $f_{v_{p,r,k},p}(q) \neq 1$ and $f_{v_{p,r,k},r}(q) \neq 1$. Therefore $s_{p,k} = s_{r,k} = 1$. Let $f_p(q) = \prod_j f_{u_{p,j},p}(q)$ where $f_{u_{p,j},p}(q)$ is the factor of $f_p(q)$ such that its roots are all the roots of $f_p(q)$ which are primitive $u_{p,j}p$-roots of unity. Let L be the positive integer $u_{p,l}$ where $u_{p,l} = v_{p,r,k}$. Since $u_{p,l}$ is independent of r, the result follows. □

Let p_m, p_n be any two distinct primes. Let $\square$ denote either p_m or p_n. For each i, let $m_{\square,i}$ be the nonnegative integer such that $(P_{v_{p_m,p_n,i},\square}(q))^{m_{\square,i}}$ is the highest power of $P_{v_{p_m,p_n,i},\square}(q)$ dividing $f_{v_{p_m,p_n,i},\square}(q)$.

Proposition 3.25 *(Key Proposition 4). Let p be the prime chosen in part* (1) *of Key Proposition* 2. *Let r be any prime. Let $k := k_{p,r}$ be the integer defined in Key Proposition* 2. *Let $e_{1,r}$ be defined as in Key Proposition* 2. *Then the following statements hold*:

(a) *If r is not in $\mathcal{U}$ or if r is in $\mathcal{U}$ and $e_{1,r} < k$, then $\frac{f_p(q)}{\prod_{i<k}(P_{v_{p,r,i},p}(q))^{m_{p,i}}}$ and $\frac{f_r(q)}{\prod_{i<k}(P_{v_{p,r,i},r}(q))^{m_{r,i}}}$ satisfy Functional Equation* (1).

(b) *If r is in $\mathcal{U}$ and $e_{1,r} < k$, define*:

- $n_{p,e_{1,r}} = m_{p,e_{1,r}}$.
- $n_{p,e_{i,r}} = n_{p,e_{i-1,r}} + m_{r,e_{i,r}}$ *for* $1 < i \leqslant b_r$.

Then

$$\frac{f_p(q)}{\prod_{i\leqslant e_{1,r}}(P_{v_{p,r,i},p}(q))^{m_{p,i}}\prod_{1<i\leqslant b_r}(P_{v_{p,r,e_{i,r}},p}(q))^{n_{p,e_{i,r}}}}$$

and

$$\frac{f_r(q)}{\prod_{i\leqslant e_{1,r}}(P_{v_{p,r,i},r}(q))^{m_{r,i}}\prod_{1<i\leqslant b_r}(P_{v_{p,r,e_{i,r}},r}(q))^{m_{r,e_{i,r}}}}$$

satisfy Functional Equation (1).

Proof. (a) If r is not in $\mathcal{U}$ or if $e_{1,r}\geqslant k$, then p and r do not divide $v_{p,r,i}$ for any bi-level $i<k$. It follows from the minimality of k as well as parts (a) and (b) of Key Proposition 2 that the reduced form of EFE(1) with respect to p and r has the form

$$\begin{array}{ccc}
\dfrac{(P_{v_{p,r,1},r}(q^p))^{m_{r,1}}}{(P_{v_{p,r,1},r}(q))^{m_{r,1}}} & \overset{(1)}{\longleftrightarrow} & \dfrac{(P_{v_{p,r,1},p}(q^r))^{m_{p,1}}}{(P_{v_{p,r,1},p}(q))^{m_{p,1}}}\\
\cdots & \cdots & \cdots\\
\dfrac{(P_{v_{p,r,k-1},r}(q^p))^{m_{r,k-1}}}{(P_{v_{p,r,k-1},r}(q))^{m_{r,k-1}}} & \overset{(k-1)}{\longleftrightarrow} & \dfrac{(P_{v_{p,r,k-1},p}(q^r))^{m_{p,k-1}}}{(P_{v_{p,r,k-1},p}(q))^{m_{p,k-1}}}\\
f_{v_{p,r,k},p}(q)^{s_{p,k}\delta_{r,k}}\dfrac{f_{v_{p,r,k},r}(q^p)^{s_{r,i}}}{f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}(1-\delta_{p,k})}} & \overset{(k)}{\longleftrightarrow} & f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}\delta_{p,k}}\dfrac{f_{v_{p,r,k},p_0}(q^r)^{s_{v_{p,k}}}}{f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}(1-\delta_{r,k})}}\\
\cdots & \cdots & \cdots\\
Q_{p,r}(q) & = & Q_{p,r}(q).
\end{array}$$

It can be verified that $\overset{(i)}{\longleftrightarrow}$ can be replaced by $\overset{(i)}{=}$ for each $i\in\{1,\dots,k-1\}$. Hence

$$\prod_{1\leqslant i\leqslant k-1}\frac{(P_{v_{p,r,i},r}(q^p))^{m_{r,i}}}{(P_{v_{p,r,i},r}(q))^{m_{r,i}}}=\prod_{1\leqslant i\leqslant k-1}\frac{(P_{v_{p,r,i},p}(q^r))^{m_{p,i}}}{(P_{v_{p,r,i},p}(q))^{m_{p,i}}}.$$

Let us divide the left-hand side and the right-hand side of the reduced form of EFE(1) with respect to p and r above by

$$\prod_{1\leqslant i\leqslant k-1}\frac{(P_{v_{p,r,i},r}(q^p))^{m_{r,i}}}{(P_{v_{p,r,i},r}(q))^{m_{r,i}}}$$

and

$$\prod_{1\leqslant i\leqslant k-1}\frac{(P_{v_{p,r,i},p}(q^r))^{m_{p,i}}}{(P_{v_{p,r,i},p}(q))^{m_{p,i}}}$$

respectively. It can be verified that the result,

$$\begin{array}{ccc} f_{v_{p,r,k},p}(q)^{s_{p,k}\delta_{r,k}}\dfrac{f_{v_{p,r,k},r}(q^p)^{s_{r,i}}}{f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}(1-\delta_{p,k})}} & \overset{(k)}{\longleftrightarrow} & f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}\delta_{p,k}}\dfrac{f_{v_{p,r,k},p_0}(q^r)^{s_{v_{p,k}}}}{f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}(1-\delta_{r,k})}} \\ \cdots & \cdots & \cdots \\ \dfrac{Q_{p,r}(q)}{\prod_{1\leqslant i\leqslant k-1}\frac{(P_{v_{p,r,i},r}(q^p))^{m_{r,i}}}{(P_{v_{p,r,i},r}(q))^{m_{r,i}}}} & = & \dfrac{Q_{p,r}(q)}{\prod_{1\leqslant i\leqslant k-1}\frac{(P_{v_{p,r,i},p}(q^r))^{m_{p,i}}}{(P_{v_{p,r,i},p}(q))^{m_{p,i}}}} \end{array}$$

is the reduced form of EFE(1) of $\frac{f_p(q)}{\prod_{i<k}(P_{v_{p,r,i},p}(q))^{m_{p,i}}}$ and $\frac{f_r(q)}{\prod_{i<k}(P_{v_{p,r,i},r}(q))^{m_{r,i}}}$, after the bi-level(s) $k, k+1, \ldots$ are renamed as $1, 2, \ldots$ correspondingly. In particular, the polynomials $\frac{f_p(q)}{\prod_{i<k}(P_{v_{p,r,i},p}(q))^{m_{p,i}}}$ and $\frac{f_r(q)}{\prod_{i<k}(P_{v_{p,r,i},r}(q))^{m_{r,i}}}$ satisfy Functional Equation (1). Furthermore, the value of the bi-level 1 of EFE(1) of $\frac{f_p(q)}{\prod_{i<k}(P_{v_{p,r,i},p}(q))^{m_{p,i}}}$ and $\frac{f_r(q)}{\prod_{i<k}(P_{v_{p,r,i},r}(q))^{m_{r,i}}}$ is equal to the value of the bi-level $k_{p,r}$ of EFE(1) of $f_p(q)$ and $f_r(q)$.

(b) Suppose r is in $\mathcal{U}$ and $e_{1,r} < k$. If $e_{1,r} > 1$, then it follows from part (b) of Key Proposition 2 and the minimality of k that line (1) through line $(e_{1,r}-1)$ of the reduced form of EFE(1) with respect to p and r has the form

$$\begin{array}{ccc} \dfrac{(P_{v_{p,r,1},r}(q^p))^{m_{r,1}}}{(P_{v_{p,r,1},r}(q))^{m_{r,1}}} & \overset{(1)}{\longleftrightarrow} & \dfrac{(P_{v_{p,r,1},p}(q^r))^{m_{p,1}}}{(P_{v_{p,r,1},p}(q))^{m_{p,1}}} \\ \cdots & \cdots & \cdots \\ \dfrac{(P_{v_{p,r,e_{1,r}-1},r}(q^p))^{m_{r,e_{1,r}-1}}}{(P_{v_{p,r,e_{1,r}-1},r}(q))^{m_{r,e_{1,r}-1}}} & \overset{(e_{1,r}-1)}{\longleftrightarrow} & \dfrac{(P_{v_{p,r,e_{1,r}-1},p}(q^r))^{m_{p,e_{1,r}-1}}}{(P_{v_{p,r,e_{1,r}-1},p}(q))^{m_{p,e_{1,r}-1}}}. \end{array}$$

It can be verified that $\overset{(i)}{\longleftrightarrow}$ can be replaced by $\overset{(i)}{=}$ for each $i \in \{1, \ldots, e_{1,r}-1\}$. Hence

$$\prod_{1\leqslant 1\leqslant e_{1,r}-1}\frac{(P_{v_{p,r,i},r}(q^p))^{m_{r,i}}}{(P_{v_{p,r,i},r}(q))^{m_{r,i}}} = \prod_{1\leqslant 1\leqslant e_{1,r}-1}\frac{(P_{v_{p,r,i},p}(q^r))^{m_{p,i}}}{(P_{v_{p,r,i},p}(q))^{m_{p,i}}}.$$

By applying a similar argument as in part (a), it can be verified that the polynomials $\frac{f_p(q)}{\prod_{1\leqslant 1\leqslant e_{1,r}-1}(P_{v_{p,r,i},p}(q))^{m_{p,i}}}$ and $\frac{f_r(q)}{\prod_{1\leqslant 1\leqslant e_{1,r}-1}(P_{v_{p,r,i},r}(q))^{m_{r,i}}}$ satisfy Functional Equation (1). As a result, we may assume that $e_{1,r} = 1$.

By part (b) of Key Proposition 2, the reduced form of EFE(1) of the polynomials $f_p(q)$ and $f_r(q)$ has the form

$$\begin{array}{ccc} f_{u,p}(q)\dfrac{f_{u,r}(q^p)}{f_{u,r}(q)} & \overset{(1=e_{1,r})}{\longleftrightarrow} & f_{u,p}(q^r) \\ \cdots & \cdots & \cdots \\ f_{\frac{u}{r},p}(q)\dfrac{f_{\frac{u}{r},r}(q^p)^{s_{r,e_{2,r}}}}{f_{\frac{u}{r},r}(q)^{s_{r,e_{2,r}}}} & \overset{(e_{2,r})}{\longleftrightarrow} & f_{\frac{u}{r},p}(q^r) \\ \cdots & \cdots & \cdots \\ f_{\frac{u}{r^2},p}(q)\dfrac{f_{\frac{u}{r^2},r}(q^p)^{s_{r,e_{3,r}}}}{f_{\frac{u}{r^2},r}(q)^{s_{r,e_{3,r}}}} & \overset{(e_{3,r})}{\longleftrightarrow} & f_{\frac{u}{r^2},p}(q^r) \\ \cdots & \cdots & \cdots \end{array}$$

$$\begin{array}{ccc} \dfrac{f_{\frac{u}{r^{b_r}},r}(q^p)^{s_{r,e_{b_r+1,r}}}}{f_{\frac{u}{r^{b_r}},r}(q)^{s_{r,e_{b_r+1,r}}}} & \overset{(e_{b_r+1,r})}{\longleftrightarrow} & \dfrac{f_{\frac{u}{r^{b_r}},p}(q^r)}{f_{\frac{u}{r^{b_r}},p}(q)} \\ \cdots & \cdots & \cdots \\ Q_{p,r}(q) & = & Q_{p,r}(q) \end{array}$$

where $e_{2,r},\dots,e_{b_r+1,r}$ are the bi-levels of EFE(1) with respect to p and r having values $\frac{u}{r},\dots,\frac{u}{r^{b_r}}$ correspondingly.

Lemma 3.26. *The following equalities hold*:

(1) $$\frac{f_{u,r}(q^p)}{f_{u,r}(q)} = f_{u,p}\big(q^r\big).$$

(2) $$f_{u,p}(q)\frac{f_{\frac{u}{r},r}(q^p)^{s_{r,e_{2,r}}}}{f_{\frac{u}{r},r}(q)^{s_{r,e_{2,r}}}} = f_{\frac{u}{r},p}\big(q^r\big).$$

(3) $$f_{\frac{u}{r},p}(q)\frac{f_{\frac{u}{r^2},r}(q^p)^{s_{r,e_{3,r}}}}{f_{\frac{u}{r^2},r}(q)^{s_{r,e_{3,r}}}} = f_{\frac{u}{r^2},p}\big(q^r\big).$$

(4) $$f_{\frac{u}{r^2},p}(q)\frac{f_{\frac{u}{r^3},r}(q^p)^{s_{r,e_{4,r}}}}{f_{\frac{u}{r^3},r}(q)^{s_{r,e_{4,r}}}} = f_{\frac{u}{r^3},p}\big(q^r\big).$$

$$\cdots$$

(b_r) $$f_{\frac{u}{r^{b_r-1}},p}(q)\frac{f_{\frac{u}{r^{b_r}},r}(q^p)^{s_{r,e_{b_r+1,r}}}}{f_{\frac{u}{r^{b_r}},r}(q)^{s_{r,e_{b_r+1,r}}}} = \frac{f_{\frac{u}{r^{b_r}},p}(q^r)}{f_{\frac{u}{r^{b_r}},p}(q)}.$$

Proof. (1) It can be verified that $\frac{f_{u,r}(q^p)}{f_{u,r}(q)}$ and $f_{u,p}(q^r)$ are the factors of $f_p(q)f_r(q^p)$ and $f_r(q)f_p(q^r)$ respectively whose roots are all the roots of $f_p(q)f_r(q^p)$ and $f_r(q)f_p(q^r)$ respectively which are primitive upr-roots of unity. Since

$$f_p(q)f_r\big(q^p\big) = f_r(q)f_p\big(q^r\big),$$

the result follows.

Similarly, (2), (3), …, (b_r) follows since the left-hand sides and the right-hand sides of (2), (3), …, (b_r) are the factors of $f_p(q)f_r(q^p)$ and $f_r(q)f_p(q^r)$ respectively whose roots are all the roots of $f_p(q)f_r(q^p)$ and $f_r(q)f_p(q^r)$ respectively which are primitive upr^0-roots of unity, primitive upr^{-1}-roots of unity, …, primitive $upr^{-(b_r-1)}$-roots of unity correspondingly. □

It follows from the assumption $e_{1,r} < k$ and the minimality of k that

$$P_{upr}(q)^{m_{r,1}} = \frac{P_{u,r}(q^p)^{m_{r,1}}}{P_{u,r}(q)^{m_{r,1}}} = \frac{f_{u,r}(q^p)}{f_{u,r}(q)} = f_{u,p}\big(q^r\big) = P_{u,p}\big(q^r\big)^{m_{p,1}} = P_{upr}(q)^{m_{p,1}},$$

where $P_{upr}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ and order upr. Hence $m_{p,1} = m_{r,1}$.

By definition of $m_{p,1}$ and $m_{r,e_{2,r}}$, there exist polynomials $f'_{u,p}(q)$ and $f'_{\frac{u}{r},r}(q)$ such that

$$f_{u,p}(q) = \big(P_{u,p}(q)\big)^{m_{p,1}} f'_{u,p}(q)$$

and

$$f_{\frac{u}{r},r}(q) = \big(P_{\frac{u}{r},r}(q)\big)^{m_{r,e_{2,r}}} f'_{\frac{u}{r},r}(q).$$

Hence

$$\begin{aligned} f_{u,p}(q)\frac{f_{\frac{u}{r},r}(q^p)^{s_{r,e_{2,r}}}}{f_{\frac{u}{r},r}(q)^{s_{r,e_{2,r}}}} &= \big(P_{u,p}(q)\big)^{m_{p,1}} f'_{u,p}(q)\frac{(P_{\frac{u}{r},r}(q^p))^{m_{r,e_{2,r}}} f'_{\frac{u}{r},r}(q^p)}{(P_{\frac{u}{r},r}(q))^{m_{r,e_{2,r}}} f'_{\frac{u}{r},r}(q)} \\ &= \big(P_{u,p}(q)\big)^{m_{p,1}} \frac{(P_{\frac{u}{r},r}(q^p))^{m_{r,e_{2,r}}}}{(P_{\frac{u}{r},r}(q))^{m_{r,e_{2,r}}}} f'_{u,p}(q)\frac{f'_{\frac{u}{r},r}(q^p)}{f'_{\frac{u}{r},r}(q)} \\ &= \big(P_{u,p}(q)\big)^{m_{p,1}+m_{r,e_{2,r}}} f'_{u,p}(q)\frac{f'_{\frac{u}{r},r}(q^p)}{f'_{\frac{u}{r},r}(q)} = \big(P_{u,p}(q)\big)^{n_{p,e_{2,r}}} f'_{u,p}(q)\frac{f'_{\frac{u}{r},r}(q^p)}{f'_{\frac{u}{r},r}(q)}. \end{aligned}$$

Hence

$$f_{\frac{u}{r},p}\big(q^r\big) = \big(P_{u,p}(q)\big)^{n_{p,e_{2,r}}} f'_{\frac{u}{r},p}\big(q^r\big)$$

for some polynomial $f'_{\frac{u}{r},p}(q^r)$.

By similar arguments, it can be verified that there exist collections of polynomials

$$\begin{gathered} \big\{f'_{\frac{u}{r},p}(q), f'_{\frac{u}{r^2},r}(q), f'_{\frac{u}{r^2},p}(q)\big\}, \\ \big\{f'_{\frac{u}{r^2},p}(q), f'_{\frac{u}{r^3},r}(q), f'_{\frac{u}{r^3},p}(q)\big\}, \\ \cdots \\ \big\{f'_{\frac{u}{r^{br-1}},p}(q), f'_{\frac{u}{r^{br}},r}(q), f'_{\frac{u}{r^{br}},p}(q)\big\} \end{gathered}$$

such that

$$\begin{aligned} \big(P_{\frac{u}{r},p}(q)\big)^{n_{p,e_{3,r}}} f'_{\frac{u}{r},p}(q)\frac{f'_{\frac{u}{r^2},r}(q^p)^{s_{r,e_{3,r}}}}{f'_{\frac{u}{r^2},r}(q)^{s_{r,e_{3,r}}}} &= f_{\frac{u}{r},p}(q)\frac{f_{\frac{u}{r^2},r}(q^p)^{s_{r,e_{3,r}}}}{f_{\frac{u}{r^2},r}(q)^{s_{r,e_{3,r}}}} = f_{\frac{u}{r^2},p}\big(q^r\big) \\ &= \big(P_{\frac{u}{r},p}(q)\big)^{n_{p,e_{3,r}}} f'_{\frac{u}{r^2},p}\big(q^r\big), \\ \big(P_{\frac{u}{r^2},p}(q)\big)^{n_{p,e_{4,r}}} f'_{\frac{u}{r^2},p}(q)\frac{f'_{\frac{u}{r^3},r}(q^p)^{s_{r,e_{4,r}}}}{f'_{\frac{u}{r^3},r}(q)^{s_{r,e_{4,r}}}} &= f_{\frac{u}{r^2},p}(q)\frac{f_{\frac{u}{r^3},r}(q^p)^{s_{r,e_{4,r}}}}{f_{\frac{u}{r^3},r}(q)^{s_{r,e_{4,r}}}} = f_{\frac{u}{r^3},p}\big(q^r\big) \\ &= \big(P_{\frac{u}{r^2},p}(q)\big)^{n_{p,e_{4,r}}} f'_{\frac{u}{r^3},p}\big(q^r\big), \\ &\cdots \end{aligned}$$

$$\left(P_{\frac{u}{r^{b_r-1}},p}(q)\right)^{n_{p,e_{b_r+1,r}}} f'_{\frac{u}{r^{b_r-1}},p}(q)\frac{f'_{\frac{u}{r^{b_r}},r}(q^p)^{s_{r,e_{b_r+1,r}}}}{f'_{\frac{u}{r^{b_r}},r}(q)^{s_{r,e_{b_r+1,r}}}} = f_{\frac{u}{r^{b_r-1}},p}(q)\frac{f_{\frac{u}{r^{b_r}},r}(q^p)^{s_{r,e_{b_r+1,r}}}}{f_{\frac{u}{r^{b_r}},r}(q)^{s_{r,e_{b_r+1,r}}}}$$

$$= \frac{f_{\frac{u}{r^{b_r}},p}(q^r)}{f_{\frac{u}{r^{b_r}},p}(q)} = \left(P_{\frac{u}{r^{b_r-1}},p}(q)\right)^{n_{p,e_{b_r+1,r}}}\frac{f'_{\frac{u}{r^{b_r}},p}(q^r)}{f'_{\frac{u}{r^{b_r}},p}(q)},$$

where

$$n_{p,e_{i,r}} = n_{p,e_{i-1,r}} + m_{r,e_{i,r}}$$

for $i \in \{3,\dots,b_r+1\}$.

By replacing

$$\left\{f_{\frac{u}{r},p}(q), f_{\frac{u}{r^2},r}(q), f_{\frac{u}{r^2},p}(q)\right\},$$
$$\left\{f_{\frac{u}{r^2},p}(q), f_{\frac{u}{r^3},r}(q), f_{\frac{u}{r^3},p}(q)\right\},$$
$$\dots$$
$$\left\{f_{\frac{u}{r^{b_r-1}},p}(q), f_{\frac{u}{r^{b_r}},r}(q), f_{\frac{u}{r^{b_r}},p}(q)\right\}$$

with

$$\left\{f'_{\frac{u}{r},p}(q), f'_{\frac{u}{r^2},r}(q), f'_{\frac{u}{r^2},p}(q)\right\},$$
$$\left\{f'_{\frac{u}{r^2},p}(q), f'_{\frac{u}{r^3},r}(q), f'_{\frac{u}{r^3},p}(q)\right\},$$
$$\dots$$
$$\left\{f'_{\frac{u}{r^{b_r-1}},p}(q), f'_{\frac{u}{r^{b_r}},r}(q), f'_{\frac{u}{r^{b_r}},p}(q)\right\}$$

in EFE(1) of $f_p(q)$ and $f_r(q)$ correspondingly and eliminating line $(e_{1,r})$, it can be verified that the result is EFE(1) of

$$\frac{f_p(q)}{\prod_{i\leqslant e_{1,r}}(P_{v_{p,r,i},p}(q))^{m_{p,i}}\prod_{1<i\leqslant b_r}(P_{v_{p,r,e_{i,r}},p}(q))^{n_{p,e_{i,r}}}}$$

and

$$\frac{f_r(q)}{\prod_{i\leqslant e_{1,r}}(P_{v_{p,r,i},r}(q))^{m_{r,i}}\prod_{1<i\leqslant b_r}(P_{v_{p,r,e_{i,r}},r}(q))^{m_{r,e_{i,r}}}}.$$

As a result,

$$\frac{f_p(q)}{\prod_{i\leqslant e_{1,r}}(P_{v_{p,r,i},p}(q))^{m_{p,i}}\prod_{1<i\leqslant b_r}(P_{v_{p,r,e_{i,r}},p}(q))^{n_{p,e_{i,r}}}}$$

and

$$\frac{f_r(q)}{\prod_{i\leqslant e_{1,r}}(P_{v_{p,r,i},r}(q))^{m_{r,i}}\prod_{1<i\leqslant b_r}(P_{v_{p,r,e_{i,r}},r}(q))^{m_{r,e_{i,r}}}}$$

satisfy Functional Equation (1). □

If case (a) of Key Proposition 4 occurs, we replace the polynomials $f_p(q)$ and $f_r(q)$ by the polynomials $\frac{f_p(q)}{\prod_{i<k}(P_{v_{p,r,i},p}(q))^{m_{p,i}}}$ and $\frac{f_r(q)}{\prod_{i<k}(P_{v_{p,r,i},r}(q))^{m_{r,i}}}$ respectively. Let us denote the latter polynomials also by $f_p(q)$ and $f_r(q)$ respectively. Let $k_{p,r}$ be the positive integer defined in Key Proposition 2 for the new polynomials $f_p(q)$ and $f_r(q)$. It can be verified that $k_{p,r}=1$. As indicated in the proof of (a) above, the value of the bi-level 1 of EFE(1) of $\frac{f_p(q)}{\prod_{i<k}(P_{v_{p,r,i},p}(q))^{m_{p,i}}}$ and $\frac{f_r(q)}{\prod_{i<k}(P_{v_{p,r,i},r}(q))^{m_{r,i}}}$ is equal to the value of the bi-level $k_{p,r}$ of $f_p(q)$ and $f_r(q)$.

If case (b) occurs, we replace the polynomials $f_p(q)$ and $f_r(q)$ by the polynomials

$$\frac{f_p(q)}{\prod_{i\leqslant e_{1,r}}(P_{v_{p,r,i},p}(q))^{m_{p,i}}\prod_{1<i\leqslant b_r}(P_{v_{p,r,e_{i,r}},p}(q))^{n_{p,e_{i,r}}}}$$

and

$$\frac{f_r(q)}{\prod_{i\leqslant e_{1,r}}(P_{v_{p,r,i},r}(q))^{m_{r,i}}\prod_{1<i\leqslant b_r}(P_{v_{p,r,e_{i,r}},r}(q))^{m_{r,e_{i,r}}}}.$$

Let us also denote the latter polynomials by $f_p(q)$ and $f_r(q)$ respectively. Let $k_{p,r}$ be the positive integer defined in Key Proposition 2 for the new polynomials $f_p(q)$ and $f_r(q)$. If $k_{p,r}\neq 1$, repeat the process in part (a) or (b) of Key Proposition 4 above with $\frac{f_p(q)}{\prod_{i\leqslant e_{1,r}}(P_{v_{p,r,i},p}(q))^{m_{p,i}}\prod_{1<i\leqslant b_r}(P_{v_{p,r,e_{i,r}},p}(q))^{n_{p,e_{i,r}}}}$ and $\frac{f_r(q)}{\prod_{i\leqslant e_{1,r}}(P_{v_{p,r,i},r}(q))^{m_{r,i}}\prod_{1<i\leqslant b_r}(P_{v_{p,r,e_{i,r}},r}(q))^{m_{r,e_{i,r}}}}$ replacing $f_p(q)$ and $f_r(q)$ respectively. It is straightforward to verify that $k_{p,r}=1$ eventually (we leave the details to readers) and that the value of the bi-level 1 of EFE(1) of the resulting polynomials is equal to the value of the bi-level $k_{p,r}$ of $f_p(q)$ and $f_r(q)$.

Proposition 3.27 *(Key Proposition 5). Let p be the prime chosen in the proof of Key Proposition* 2 *and r be any prime. Let $k=k_{p,r}$ be the smallest bi-level of* EFE(1) *with respect to p and r such that the coefficients of either $f_{v_{p,r,k},p}(q)$ or $f_{v_{p,r,k},r}(q)$ are not properly contained in $\mathbb{Q}$. Then*

$$v_{p,r,k}>1.$$

Proof. Since $v_{p,r,k}=L$ all primes r by Key Proposition 2, we may assume without loss of generality that r is not in $\mathcal{U}$. Hence r does not divide $v_{p,r,k}$. By Key Proposition 4, we may assume, without loss of generality, in the rest of the proof of this proposition that $k=1$. As a result, $f_{v_{p,r,1},p}(q)$ and $f_{v_{p,r,1},r}(q)$ are super-compatible by Key Proposition 1′.

Since $f_{v_{p,r,1},p}(q)$ and $f_{v_{p,r,1},r}(q)$ are super-compatible, they can be written as $f_{v_{p,r,1},p}(q)=\prod_i(F^{(i)}_{v_{p,r,1},p}(q))^{n_i}$ and $f_{v_{p,r,1},r}(q)=\prod_i(F^{(i)}_{v_{p,r,1},r}(q))^{n_i}$, where $F^{(i)}_{v_{p,r,1},p}(q)$ and $F^{(i)}_{v_{p,r,1},r}(q)$ are polynomials which are compatible for each i. Since the coefficients of $f_{v_{p,r,1},p}(q)$ and $f_{v_{p,r,1},r}(q)$ are not properly contained in $\mathbb{Q}$, there exists at least one index i such that the coefficients of $F^{(i)}_{v_{p,r,1},p}(q)$ are not properly contained in $\mathbb{Q}$. Hence the coefficients of $F^{(i)}_{v_{p,r,1},r}(q)$ are also not properly contained in $\mathbb{Q}$ (see that proof of Key Proposition 1). Therefore, $v_{p_n,p_m,k}>1$ by Key Proposition 1. □

Proposition 3.28 *(Key Proposition 6). Let p be as defined in the proof of Key Proposition 2 and r be any prime such that r does not divide $v_{p,r,k_{p,r}}$. Then*

$$v_{p,r,k_{p,r}} = 2.$$

Proof. Let us recall that there exists a positive integer L such that $v_{p,r,k_{p,r}} = L$ for all primes r by part (3) of Key Proposition 2. From the definition of $k_{p,r}$ (see part (2) of Key Proposition 2), the coefficients of $f_{v_{p,r,k_{p,r}},p}(q)$ and $f_{v_{p,r,k_{p,r}},r}(q)$ are not properly contained in $\mathbb{Q}$. Suppose $L > 2$. Then $(\mathbb{Z}/L\mathbb{Z})^*$ contains at least one nonempty proper subset. Choose the prime r so that r does not divide L. Since we are interested in the value of the bi-level $k_{p,r}$, we may assume without loss of generality that $k_{p,r} = 1$ by Key Proposition 4. Thus line $(k_{p,r})$ of the reduced form of EFE(1) with respect to p and r has the form

$$\frac{f_{v_{p,r,k_{p,r}},r}(q^p)}{f_{v_{p,r,k_{p,r}},r}(q)} \overset{(k_{p,r})}{\longleftrightarrow} \frac{f_{v_{p,r,k_{p,r}},p}(q^r)}{f_{v_{p,r,k_{p,r}},p}(q)}.$$

Let

$$\frac{f_{v_{p,r,k_{p,r}},p}(q^r)}{f_{v_{p,r,k_{p,r}},p}(q)} = \prod_{0 \leqslant j \leqslant z} \left(\frac{\pi^{(j)}_{v_{p,r,k_{p,r}},p}(q^r)}{\pi^{(j)}_{v_{p,r,k_{p,r}},p}(q)} \right)^{e_j}$$

be the factorization defined in Key Proposition $1'$ and its proof. Then

$$\frac{f_{v_{p,r,k_{p,r}},p}(q^r)}{f_{v_{p,r,k_{p,r}},p}(q)}$$

and thus

$$\frac{\pi^{(j)}_{v_{p,r,k_{p,r}},p}(q^r)}{\pi^{(j)}_{v_{p,r,k_{p,r}},p}(q)}$$

is a polynomial for each j. Let $\mathcal{A}_j$ be defined as in the proof of Key Proposition $1'$. Then

$$r\mathcal{A}_0 = \mathcal{A}_0.$$

Recall from the proof of Key Proposition $1'$ that we may assume that $\mathcal{A}_0$ is a nonempty proper subset of $(\mathbb{Z}/v_{p,r,k_{p,r}}\mathbb{Z})^*$ (otherwise, replace $\mathcal{A}_0$ by the smallest index j such that $\mathcal{A}_j$ is a nonempty proper subset of $(\mathbb{Z}/v_{p,r,k_{p,r}}\mathbb{Z})^*$). Let α_L be an element of $(\mathbb{Z}/v_{p,r,k_{p,r}}\mathbb{Z})^* - \mathcal{A}_0 = (\mathbb{Z}/L\mathbb{Z})^* - \mathcal{A}_0$. There are two cases:

(1) 1 is in $\mathcal{A}_0$.
(2) 1 is not in $\mathcal{A}_0$.

If (1) is the case, then we can choose r so that r also satisfy

$$r = r.1 \equiv \alpha_L \pmod{L}$$

by Dirichlet prime numbers in arithmetic sequences. This is a contradiction since $r\mathcal{A}_0 = \mathcal{A}_0$.

If (2) occurs, then we can choose r so that r also satisfy

$$r = r.1 \equiv \alpha_L \pmod{L}$$

by the same reason. This is also a contradiction since $r\mathcal{A}_0 = \mathcal{A}_0$ implies that

$$r\big((\mathbb{Z}/L\mathbb{Z})^* - \mathcal{A}_0\big) = (\mathbb{Z}/L\mathbb{Z})^* - \mathcal{A}_0$$

since $r(\mathbb{Z}/L\mathbb{Z})^* = (\mathbb{Z}/L\mathbb{Z})^*$. As a result,

$$v_{p,r,k_{p,r}} = L = 2. \qquad \square$$

The conclusion of the proof of **Part 2** of Theorem 2.1.

Let p be the prime chosen in the proof of Key Proposition 2 and let r be another prime which is not in $\mathcal{U}$. Thus p and r do not divide $v_{p,r,i}$ for any bi-level i of EFE(1) with respect to p and r. Let us consider EFE(1) with respect to p and r. Let $k_{p,r}$ be the integer defined in Key Proposition 2, i.e. $k_{p,r}$ is the smallest positive integer such that the coefficients of $f_{v_{p,r,k_{p,r}},p}$ and $f_{v_{p,r,k_{p,r}},r}$ are not properly contained in $\mathbb{Q}$. By Key Proposition 4, we may assume that $k_{p,r} = 1$. Therefore, $f_{v_{p,r,k_{p,r}},p}(q)$ and $f_{v_{p,r,k_{p,r}},r}(q)$ are super-compatible by Key Proposition 1′. Since $v_{p,r,k_{p,r}} = 2$, $f_{2,p}(q)$ and $f_{2,r}(q)$ are supper-compatible. As a result, there exists a subset $\mathcal{A}_2$ of $((\mathbb{Z}/2\mathbb{Z})^*)^T$, for some positive integer T, such that roots of $f_{2,p}(q)$ and $f_{2,r}(q)$ are represented by the collection of tuples

$$\bigcup_{\alpha\in\mathcal{A}_2} \{\alpha\} \times (\mathbb{Z}/p\mathbb{Z})^*$$

and

$$\bigcup_{\alpha\in\mathcal{A}_2} \{\alpha\} \times (\mathbb{Z}/r\mathbb{Z})^*$$

respectively.

Since $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$,

$$\mathcal{A}_2 = \big((\mathbb{Z}/2\mathbb{Z})^*\big)^{T'}$$

for some integer $T' \leqslant T$. It can be verified that the monic polynomial whose roots are primitive $2p$-roots of unity and the monic polynomial whose roots are primitive $2r$-roots of unity represented by the collection of tuples

$$\bigcup_{\alpha\in(\mathbb{Z}/2\mathbb{Z})^*} \{\alpha\} \times (\mathbb{Z}/p\mathbb{Z})^*$$

and

$$\bigcup_{\alpha\in(\mathbb{Z}/2\mathbb{Z})^*} \{\alpha\} \times (\mathbb{Z}/r\mathbb{Z})^*$$

respectively are the cyclotomic polynomial, with coefficients in $\mathbb{Q}$ of order $2p$, $P_{2p}(q)$ and the cyclotomic polynomial, with coefficients in $\mathbb{Q}$ of order $2r$, $P_{2r}(q)$. As a result,

$$f_{2,p}(q) = P_{2p}(q)^{T'}$$

and

$$f_{2,r}(q) = P_{2r}(q)^{T'}.$$

Therefore, the coefficients of $f_{2,p}(q)$ and $f_{2,r}(q)$ are properly contained in $\mathbb{Q}$. This is a contradiction. Therefore, the positive integer $k_{p,r}$ in part (2) of Key Proposition 2 does not exist, which means that the assumption that $\mathcal{J}_{p_c} \neq \emptyset$ is incorrect. Therefore the coefficients of every polynomial in a sequence of polynomials Γ satisfying the full hypothesis of Theorem 2.1 must be properly contained in $\mathbb{Q}$. Thus by Part 1, every element of Γ can be written as a product of quantum integers in the fashion described in Theorem 2.1. The proof of Theorem 2.1 is thus complete and constitutes a solution to Problem 1.

To give one of the important consequences of Theorem 2.1, let us assume Theorem 2.3 which is stated at the beginning. Since Theorem 2.3 is one of the main results in our next paper [2], we delay the proof to that paper which is under preparation.

Proof of Corollary 2.4. Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a sequence of polynomials with field of coefficients of characteristic zero satisfying Functional Equation (2). Let P be the set of primes associated to the support A_P of Γ. Suppose P contains at least two distinct primes.

By Theorem 2.3, there exists a sequence $\Gamma' = \{f'_n(q) \mid n \in \mathbb{N}\}$ of polynomials with field of coefficients $\mathbb{Q}$ and $\operatorname{supp}\{\Gamma\} = \operatorname{supp}\{\Gamma'\}$ such that Γ satisfies Functional Equation (2), $f_n(q)$ divides $f'_n(q)$ for all n in $\mathbb{N} \cap \operatorname{supp}\{\Gamma\}$ and $t_{\Gamma'} - t_\Gamma \in \mathbb{N}$. By Theorem 2.1, Part 1, every polynomial $f'_n(q)$ in Γ can be written in the form

$$f'_n(q) = \prod_i \left([n]_{q^{a_i}}\right)^{b_i}$$

for some collection of ordered pairs of integers $\{(a_i, b_i)_i\}$ and $t_{\Gamma'} = \sum_i a_i b_i \in \mathbb{Z}$. Since $t_{\Gamma'} - t_\Gamma \in \mathbb{N}$, t_Γ is integral as required. □

As mentioned above as well as in [1], there are sequences of polynomials satisfying Functional Equation (2) such that t_Γ can actually attain nonintegral values. The above results limit this possibility to the case where P consists of exactly one prime. As Theorem 2.5 provides a complete classification of the sequences Γ's satisfying Functional Equation (2) with t_Γ nonintegral, the problem of classification of all the sequences of polynomials solutions to Functional Equation (2) reduces to the case of integral t_Γ. Therefore Problem 2 [2] is now reduced to the cases where t_Γ is integral.

Proof of Theorem 2.5. (a) Let Γ be a sequence of polynomials with field of coefficients of characteristic zero such that Γ satisfies Functional Equation (2). Suppose t_Γ is nonintegral. It follows from Corollary 2.4 that $|P| = 1$ where P is the set of primes associated to the support A_P of Γ.

(b) Let $P = \{p\}$ where p is a prime. The support of Γ, A_P, must have the form $\{p^n \mid n \in \mathbb{N}\}$ for the prime p in P. As Γ satisfies Functional Equation (2), we have

$$f_{p^n}(q) = f_p(q) f_{p^{n-1}}\left(q^p\right)$$

for any n in $\mathbb{N}$. As a result, each polynomial $f_{p^n}(q)$ is determined by $f_p(q)$ by induction. Therefore, so is Γ.

In the opposite direction, let the triple $(f(q), p, t)$ be defined as follows:

- p is a prime and t is a positive integer.
- $f(q)$ is a monic polynomial with nonzero constant term such that $\deg(f(q)) = td$ and $(t, \frac{p-1}{d}) = 1$, where d is a proper divisor of $p-1$.

Let $f_p(q) := f(q)$, $f_1(q) = 1$ and

$$f_{p^n}(q) = f_p(q) f_{p^{n-1}}\left(q^p\right) \tag{3.3}$$

for all n in $\mathbb{N}$.

Lemma 3.29. *Let n be any natural number. Let u and v be nonnegative integers such that $u + v = n$. Then*

$$f_{p^n}(q) = f_{p^u}(q) f_{p^v}\left(q^{p^u}\right) = f_{p^v}(q) f_{p^u}\left(q^{p^v}\right). \tag{3.4}$$

Proof. Without loss of generality, we may assume that $u \geqslant 1$ and $v \geqslant 1$ because if either of them is equal to 0, then (3.4) becomes $f_{p^n}(q) = f_{p^n}(q)$. We prove this lemma by induction on n:

(1) For $n = 2$, (3.4) becomes

$$f_{p^2}(q) = f_p(q) f_p\left(q^p\right) = f_p(q) f_p\left(q^p\right)$$

which holds because of (3.3).

(2) It can be verified from (3.3) and the induction hypothesis that

$$f_{p^n}(q) = f_p(q) f_{p^{n-1}}\left(q^p\right) = f_p(q) f_{p^{u-1}}\left(q^p\right) f_{p^v}\left(\left(q^p\right)^{p^{u-1}}\right) = f_{p^u}(q) f_{p^v}\left(q^{p^u}\right).$$

Similarly,

$$f_{p^n}(q) = f_p(q) f_{p^{n-1}}\left(q^p\right) = f_p(q) f_{p^{v-1}}\left(q^p\right) f_{p^u}\left(\left(q^p\right)^{p^{v-1}}\right) = f_{p^v}(q) f_{p^u}\left(q^{p^v}\right).$$

Therefore,

$$f_{p^n}(q) = f_{p^u}(q) f_{p^v}\left(q^{p^u}\right) = f_{p^v}(q) f_{p^u}\left(q^{p^v}\right)$$

for all nonnegative integers u and v. In particular, the sequence of polynomials

$$\Gamma := \left\{ f_{p^n}(q) \;\middle|\; n \in \mathbb{N} \right\}$$

satisfies Functional Equation (2). □

As a result of Lemma 3.29, there exists a rational number t_Γ such that

$$\deg\left(f_p(q)\right) = t_\Gamma (p-1)$$

by [1]. Since d is a proper divisor of $p-1$, $\frac{p-1}{d} > 1$. Hence, $\frac{t}{\frac{p-1}{d}}$ is not integral since $(t, \frac{p-1}{d}) = 1$. Therefore,

$$\deg\left(f_p(q)\right) = td = \frac{t}{\frac{p-1}{d}}(p-1).$$

This implies that $t_\Gamma = \frac{t}{\frac{p-1}{d}}$ and thus is not integral. Therefore, the triple described above, namely

$$\left(f(q), p, t\right),$$

determines a sequence of polynomials Γ satisfying Functional Equation (2) with t_Γ nonintegral and support base $P = \{p\}$ such $f_p(q) = f(q)$. For uniqueness, let suppose that there exist positive integer t_1 and d_1 such that $\deg(f(q)) = t_1 d_1$ and $t_1 \neq t$ (thus $d_1 \neq d$ as well), where d_1 is a proper divisor of $p-1$ such that $(t_1, \frac{p-1}{d_1}) = 1$. Since $t_1 \neq t$, we may assume that $t_1 > t$. As $t_1 d_1 = td$,

$$\frac{t_1}{t} = \frac{d}{d_1}.$$

Let u, v be positive integers such that $(u, v) = 1$ and $\frac{u}{v} = \frac{t_1}{t} = \frac{d}{d_1}$. Then $u > v$. Thus there exists at least one prime, say s such that s divides u. Hence s divides t_1. Let n and m be the highest power of s dividing d and d_1 respectively. It can be verified that $n > m \geqslant 0$. Since d is a divisor of $p-1$, it follows that s divides $\frac{p-1}{d_1}$. This is a contradiction since $(t_1, \frac{p-1}{d_1}) = 1$ by assumption. Therefore $t_1 = t$ and thus $d_1 = d$. Therefore, uniqueness follows. □

Theorem 2.7 also concerns sequences of polynomials with fields of coefficients of characteristic zero satisfying Functional Equation (2) with nonintegral t_Γ. Even though it is not a part of the problems stated earlier, it is worth proving because it gives a characterization of all the sequences Γ's, with nonintegral parameter t_Γ, which can be decomposed as products of quantum integers, i.e., those which are strictly generated by quantum integers. It shows in fact that in such cases, these sequences are essentially formed by taking products of sequences of polynomials Γ_i, satisfying Functional Equation (2) and with integral parameter t_{Γ_i}, each of which is generated by quantum integers.

Proof of Theorem 2.7. Suppose that $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ is generated by quantum integers. Then there exist ordered pairs of integers $\{u_i, t_i\}_i$ such that $t_\Gamma = \sum_i u_i t_i$ and

$$f_n(q) = \prod_i \left([n]_{q^{u_i}}\right)^{t_i}$$

for each n in the support of Γ. Hence t_Γ is integral which contradicts the hypothesis of this theorem. Therefore, Γ is not generated by quantum integers.

For the statement concerning the strictly weakly generated by quantum integers, the if direction is immediate. For the only if direction, let us suppose that $f_p(q)$ is strictly weakly generated by quantum integers. Then its field of coefficients is $\mathbb{Q}$. Let α be any root of $f_p(q)$. Then α is a nontrivial root of unity. Hence its order, as a root of unity, is divisible by some prime p_i. Thus the minimal polynomial $m_\alpha(q)$ of α over the field of coefficients of Γ is $P_{up_i}(q)$ for some positive integer u, the cyclotomic polynomial with coefficients in $\mathbb{Q}$ and order up_i. Let n_i be the highest power of $P_{up_i}(q)$ dividing $f_p(q)$. From the proof of Part 1 of Theorem 2.1, $P_{up_i}(q) = \prod_j ([p_i]_{q^{a_{ij}}})^{b_{ij}}$ for some collection of ordered pairs of integers $\{(a_{ij}, b_{ij})_j\}$. As a result,

$$f_p(q) = \prod_i \left(\prod_j \left([p_i]_{q^{a_{ij}}}\right)^{b_{ij}} \right)^{n_i}.$$

Let

$$\Gamma_i := \left\{ g_{p_i^n}(q) \;\middle|\; g_{p_i}(q) = \prod_j \left([p_i]_{q^{a_{ij}}}\right)^{b_{ij}},\ n \in \mathbb{N} \right\},$$

where

$$g_{p_i^n}(q) = g_{p_i}(q) g_{p_i^{n-1}}\left(q^{p_i}\right)$$

for all n in $\mathbb{N}$. Then it can be verified that Γ_i satisfies Functional Equation (2) from the proof of Theorem 2.5. It is an immediately consequence of its definition that Γ_i is generated by quantum integers.

The uniqueness in the sense described in the statement of Theorem 2.7 follows directly from the definitions of Γ_i and n_i for each i. □

We now have a very useful tool for working with general solutions of Functional Equation (2); namely to decompose them into products of quantum integers or polynomials related to quantum integers which are more concrete and thus easier for computational as well as classification purposes. This in fact enables us to characterize all solutions of Functional Equation (2), namely Problem 2, as well as to tackle the other questions; Problem 3, Problem 4 and others. These are the goals for our next papers.

References

[1] Melvyn B. Nathanson, A functional equation arising from multiplication of quantum integers, J. Number Theory 103 (2) (2003) 214–233.
[2] Lan Nguyen, On the classification of solutions of a functional equation arising from multiplication of quantum integers, preprint.
[3] Lan Nguyen, Extensions of supports of the solutions of a functional equation arising from multiplication of quantum integers, preprint.
[4] Lan Nguyen, On the Grothendieck group associated to the collection of all solutions of a functional equation arising from multiplication of quantum integers with a given support, preprint.
[5] Lan Nguyen, Solutions with infinite support bases of a functional equation arising from multiplication of quantum integers, preprint.